FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS

Trabajo de fin de Carrera titulado:

“LA PROBLEMÁTICA EN LA REGULACIÓN JURÍDICA ANTE LA VIOLENCIA CIBERNÉTICA EN LAS REDES SOCIALES EN EL ECUADOR”

Realizado por:

Salgado Terán Byron Sebastián

Director del proyecto:

Ab. Lisa Michelle Abcarius Racines Msc.

Como requisito para la obtención del título de:

ABOGADO DE LOS TRIBUNALES DE LA REPÚBLICA DEL ECUADOR

Quito, marzo del 2022

DECLARACIÓN JURAMENTADA

Yo, BYRON SEBASTIÁN SALGADO TERÁN, con cédula de identidad # 1721238630, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Byron Sebastián Salgado Terán

C.C.: 1721238630

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

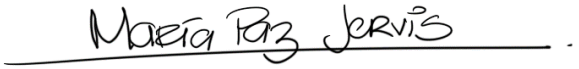
Ab. Lisa Michelle Abcarius Racines Msc.

LOS PROFESORES INFORMANTES

Ab. Fernando Javier Altamirano

Ab. María Paz Jervis Pastor

Después de revisar el trabajo presentado lo ha calificado como apto para su defensa oral ante el tribunal examinador.



Fernando Javier Altamirano Hidalgo María Paz Jervis Pastor

Quito, 15 de Marzo de 2022

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las cuentes correspondiente y en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

Byron Sebastián Salgado Terán

C.C.: 1721238630

DEDICATORIA

Dedico el presente trabajo a mi madre, a mi esposa y a mis hijas, por el apoyo brindado durante todo el tiempo que duró mis estudios.

AGRADECIMIENTO

Agradezco a toda mi familia, por haberme apoyado en el trascurso de esta etapa estudiantil, a la universidad SEK y sus profesores por haber formado un profesional con buenos valores, principios y conocimientos**.**

Resumen

El ciberacoso o acoso cibernético o conocido comúnmente como cyberbullying, que es el uso de medios tecnológicos de comunicación digital para intimidar a grupos vulnerables a través del internet utilizando las redes sociales, páginas web, blogs o aplicaciones de mensajería instantánea como WhatsApp, Instagram entre otros, que lleva a la persona a sufrir un daño repetitivo y reiterado, pues lo que se busca es crear daño, angustia, preocupación, depresión, stress, violar la intimidad personal, amenazar entre otras e incluso llevar al suicidio a la víctima, sea que esta se encuentra cerca o geográficamente distante y a cualquier hora, lo cual limita el pleno uso, goce y disfrute de sus derechos humanos.

El objetivo de esta investigación es efectuar un análisis sobre este tipo de delito informático y sus diversas formas de presentarse, así como responder a la pregunta de investigación ¿De qué manera la normativa jurídica en el país regula la violencia cibernética en las redes sociales durante el año 2020? toda vez que esta no se encuentra tipificada lo que dificulta sancionar a los agresores.

Dada la indefinición de la figura de acoso cibernético en la actual normativa legal específicamente en el Código Integral Penal, vemos que los individuos que hacen uso de las Tecnologías de Información y Comunicación o de medios digitales, se encuentran expuestas a ataques a través de las redes sociales puesto que las leyes no expresan con claridad que sanciones de deben aplicar.

Palabras claves: ciberacoso, acoso cibernético, ciberbullying, intimidación, delito, violencia cibernética, agresor, victima.

Abstract

Cyberbullying or cybernetic harassment or commonly known as cyberbullying, which is the use of technological means of digital communication to intimidate vulnerable groups through the internet using social networks, web pages, blogs or instant messaging applications such as WhatsApp, Instagram among others. others, which leads the person to suffer repetitive and repeated damage, since what is sought is to create damage, anguish, worry, depression, stress, violate personal privacy, threaten, among others, and even lead the victim to suicide, be it that it is close or geographically distant and at any time, which limits the full use, enjoyment and enjoyment of their human rights.

The objective of this research is to carry out an analysis of this type of computer crime and its various forms of presentation, as well as to answer the research question: How does the legal regulation in the country regulate cyber violence in social networks during the year 2020? since it is not typified, which makes it difficult to punish the aggressors.

Given the lack of definition of the figure of cyber bullying in the current legal regulations, specifically in the Comprehensive Criminal Code, we see that individuals who make use of Information and Communication Technologies or digital media are exposed to attacks through networks. social since the laws do not clearly express what sanctions should be applied.

Keywords: cyberbullying, cyberbullying, cyberbullying, intimidation, crime, cyber violence, aggressor, victim.

ÍNDICE

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En el Ecuador el avance y el uso de las Tecnologías de Información y Comunicación en el ciberespacio se ha convertido en un fenómeno que ha contribuido para que la sociedad cambie como lo manifiesta Mesías Narro (2008), pues el aparecimiento de nuevos medios tecnológicos han sido de gran utilidad para la humanidad toda vez que contribuyen con una mejor comunicación, transmisión de información e incluso facilitar las interrelaciones sociales, sin embargo, también han ocasionado problemas tal es el caso de la cibercriminalidad. Por otra parte, el uso del internet y las redes que se han incorporado masivamente en la vida de las personas es uno de los medios más poderosos para la comunicación y los servicios, permiten expresar ideas, recopilar información, contactarse con otros individuos, estudiar, buscar trabajo, realizar transacciones financieras, entre otras, pero también se han convertido en instrumentos nocivos como en el caso del ciberacoso donde sujetos llevan a cabo actos lesivos en contra de sus víctimas con el fin de agredir, insultar, acosar, violar la intimidad personal, amenazar, difamar, o incluso obtener lucro de estas conductas consideradas nuevos delitos informáticos que causan efectos psicológicos, emocionales y sociales para las víctimas y limitan el pleno uso, goce y disfrute de sus derechos.

En el país actualmente no existe un buen manejo de los casos de ciberacoso pues no se presta atención a las consecuencias en las víctimas, incluso no hay un adecuado tratamiento que parta desde lo educativo, sexual, de salud y legal. Aunque el Estado cuente con leyes que sancionan los delitos informáticos, muchos de ellos no se encuentran incluidos en la normativa legal de manera clara y específica así en el Código Integral Penal no se tipifica la figura del ciberacoso como delito razón por la cual se observa que existe una total desprotección para las víctimas al vulnerarse sus derechos, por ello es importante se realice un estudio a profundidad con propuestas eficientes que regulen este tipo de conducta y que permitan sancionar a los agresores.

El objetivo principal de esta investigación es identificar la problemática de la norma jurídica ecuatoriana ante el ciberacoso a través de las redes sociales,

mediante la revisión de la normativa legal relacionada que permita a futuro regular el uso de la tecnología y proteger a las personas.

El trabajo de investigación **“la problemática en la regulación jurídica ante la violencia cibernética en las redes sociales en el Ecuador** “que se presenta a continuación, consta de tres capítulo: el primer capítulo titulado violencia cibernético o ciberacoso se realiza un estudio sobre la violencia cibernética y sus características, cuales son los factores de riesgo ante el ciberacoso para finalmente abordar quienes son los protagonistas de este tipo de conducta desde los tipos de agresores, de víctimas hasta concluir con el espectador. En el segundo capítulo denominado el Internet y las redes sociales se efectúa una breve historia del internet para continuar con las redes sociales, sus características, tipo de redes, su influencia y uso, cuales con las redes más utilizadas a nivel mundial y en el Ecuador para lo cual se incluyen gráficos estadísticos y al final la regulan estas redes. En el tercero y último capítulo delito informático, ciberacoso y legislación ecuatoriana se hace alusión al concepto de delito informático y tipos, quienes son delincuentes cibernéticos, cuáles son sus objetivos y los tipos de ciberacoso, para concluir se realiza un análisis de la legislación ecuatoriana, desde la Constitución, tratados y convenios internacionales de derechos humanos y ciberdelincuencia, el Código Integral Penal, el Código de la Niñez y la Adolescencia para terminar con la Ley Orgánica de Educación Intercultural a fin de conocer las falencias de la normativa respecto de esta conducta.

CAPITULO I: VIOLENCIA CIBERNÉTICA O CIBERACOSO

Antes de hablar de violencia cibernética es importante entender el concepto de violencia así pues se la define como la coacción sea esta fuerza o violencia que se hace a una persona para precisarla que diga o ejecute alguna cosa; en otras palabras es todo acto atentatorio contra la libre voluntad de las personas en la realización de los actos jurídicos que cause daño o sufrimiento físico, sexual, psicológico, verbal, o económico a una persona. La violencia puede ser ejercida por una persona sobre otras de modo material o moral. En el primer caso, la expresión equivale a fuerza, y en el segundo, a intimidación. (Machicado, 2013).

1.1 CONCEPTUALIZACIÓN DE LA VIOLENCIA CIBERNÉTICA

No existe una definición exacta de los que es la violencia cibernética es por ello por lo que, para conceptualizar este término, se partirá de algunas definiciones que permitan aclarar que es el ciberacoso así tenemos:

Conforme el Informe Mundial sobre Violencia y la Salud emitido por la Organización Mundial de la Salud en el año 2002 la violencia se define como:

> El uso intencional de la fuerza o el poder físico, de hecho, o como amenaza, contra uno mismo, otra persona o un grupo o comunidad, que cause o tenga muchas probabilidades de causar lesiones, muerte, daños psicológicos, trastornos del desarrollo o privaciones.(Organización Mundial de la Salud. 2002. pág. 3)

Según Dupret 2012, “El término violencia deriva del latín violare: tratar con violencia, en el cual se encuentra la raíz latina vis (vires) con el sentido de fuerza en acción, fuerza ejercida contra alguien. La palabra violencia destaca la utilización de una fuerza física”. (Dupret, 2012. pág. 20)

Para Anceschi (2009) citado por Rodríguez. (2013), la violencia “es un concepto subjetivo y de definición compleja, pues adquiere varios tipos de acepciones de acuerdo con el punto de vista que se analice. Así la definición no será la misma desde una perspectiva moralista o jurídica y dentro del ámbito jurídico un

penalista no la definirá de la misma manera que un civilista. (Rodríguez, 2013. Pág. 1).

Para Vidal (2008) la violencia se definen como “la violación de la integridad de la persona “, la cual “suele ejercerse cuando interviene la fuerza física o la amenaza de su uso, pero también cuando se actúa en una secuencia que causa indefensión en el otro”, por lo que este autor la considera un proceso en el que participamos todos y no un simple acto cuyo fines la afirmación del “dominio” a través del cual busca el “control” de la presencia y las condiciones del estar, así como hacer del otro un medio considerándolo como propio y operando siempre sobre el “estar” del sujeto. (Vidal, 2008 págs. 17-20)

Respecto de la cita que antecede la violencia en el ámbito penal se podría definir como conductas cometidas en contra de otras personas, con el fin de causar un daño ya sea físico o psicológico, provocando un acto que se va en contra de la ley, la violencia desde el punto de vista penal subjetivo, siendo el Estado quien tiene la facultad para la creación de los delitos, ya que tiene la potestad de prohibir o castigar ciertas conductas que atentan en contra la de la integridad y derechos de las otras personas.

Por su parte, Matas y Alberdi 2002, citado por Rodríguez (2016) manifiestan que la violencia tiene dos condiciones fundamentales y son: la instrumentalidad y la intencionalidad, la primera no se refiere solamente a las armas sino también a los gestos, a las palabras y otras formas de expresión que logran hacen daño. La intencionalidad en cambio significa hacer un daño de forma premeditada y/o voluntaria, es lo opuesto a un hecho casual o accidental. (Rodríguez, 2016. Pág. 18).

En el derecho penal cuando se realiza un acto antijurídico (conducta que es ilícita o contraria a derecho) con el fin de causar daño de forma intencional, teniendo conocimiento y voluntad que la realización de hecho se va en contra de la ley se le conoce como dolo.

Al respecto, Zaffaroni (2006), manifiesta que el dolo es el elemento intencional, cuyo fin es causar daño, teniendo en cuenta que ese resultado se va en contra del ordenamiento jurídico. (Zaffaroni. 2006. pág. 349)

Como conclusión de los conceptos emitidos en líneas anteriores se definiría a la violencia como la realización de una gama de actos que van desde lo físico, verbal, psicológico, gestual, entre otras, que atentan contra la integridad física o psicológica con el fin de amenazar e intimidar a un individuo, comprometiendo su bienestar, de su familia y de la comunidad; desde el ámbito penal la violencia se considera como "la coerción grave, irresistible e injusta ejercida sobre una persona para determinarla contra su voluntad, a la realización de un acto jurídico" (Enciclopedia Jurídica.com. David Roger. 2020).

Hoy en día como vemos la violencia se ha esparcido en todos los ámbitos de la sociedad a través de nuevo tipos de interacciones a través del uso de medios y plataformas tecnológicas mismas que están siendo empleados para amedrantar o intimidar y victimizar a los usuarios con el propósito causarles perjuicio.

Dicho lo anterior, con la llegada de la modernidad, la globalización, la aparición del internet y las redes sociales, surge otro tipo de violencia, ya no solo de forma física sino también a través del uso de medios informáticos o digitales denominada "violencia cibernética o ciberacoso, ciberbullying ", que según el autor Enrique Mendoza López 82012) es "el acoso a través de la difusión maliciosa de información en la red, en mensajes de texto, redes sociales, correos electrónicos, en páginas web, blogs, salas de chat, etc. Puede ser información en texto, fotografías o imágenes modificadas o editadas. Todo a través de una computadora o teléfono móvil." (Enrique Mendoza López. 2012, pág. 133).

Para Sánchez, et al., (2016) El ciberacoso o ciberbullying consiste en el uso intencionado de las tecnologías de la información y la comunicación con la intención de hostigar, acosar, intimidar, insultar, molestar, vejar, humillar o amenazar. Lo que caracteriza al ciberacoso es que se trata de una conducta deliberada (no accidental), con dolo realizada a través de medios electrónicos o digitales por individuos o grupos de individuos que, de forma reiterada, envían mensajes hostiles o agresivos a otros individuos, o sobre otros individuos, con la intención de infligir daño a las víctimas. (Sánchez, et al., 2016. pág. 7).

Por su parte la UNICEF, "ciberacoso es acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de

mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a otras personas."(UNICEF. 2002)

Dorantes y Tovilla (2008), manifiestan que la "Violencia cibernética ha sido definida como el conjunto de acciones y conductas, ya sea por omisión o realización, con la finalidad de ejercer poder y control, dañando u obstaculizando la igualdad o equidad en una estructura de orden social, que cambia al relacionarse temporal y espacialmente en diferentes contextos y momentos de la historia del ser humano" (Dorantes y Tovilla, 2008. Pág. 9)

Como podemos ver la violencia cibernética o ciberacoso, no es más que el conjunto de acciones realizadas a través del uso del internet, las redes sociales, las plataformas de mensajería, o los teléfonos móviles, con el objeto de intimidar, amenazar, causar, provocar, humillar, atentar contra la intimidad de la víctima, de su familia o sus conocidos.

1.2 CARACTERÍSTICAS DEL CIBERACOSO

El acceso a internet y a través de este a las redes sociales y los mensajes de texto han contribuido para que las personas actualmente se comuniquen a diario con otras personas a un mismo tiempo lo cual ha repercutido de manera dañina en algunos casos toda vez que las nuevas formas de violencia a través del uso de los medios electrónico tienen consecuencias fatales sobre los individuos.

La violencia cibernética comúnmente llamada ciberacoso, al llevarse a cabo en el espacio virtual logra una mayor audiencia que el acoso tradicional ya que en este se concede mayor libertad de expresión y no existe el control social a las personas, de allí que varios autores consideran que para darse un acoso cibernético debe existir tres condiciones básicas ser intencional, reiterativo y provocar angustia. (Reyna-Villasmil, 2018. Pág. 190).

El ciberacoso es una conducta atemporal que genera en la victima secuelas psicológicas graves y complejas.

Examinaremos ahora de manera breve cuales con las características de la violencia cibernética o ciberacoso:

a.- Frecuencia

La frecuencia del ciberacoso es difícil de evaluar ya que puede darse con menor frecuencia con relación a otras intimidaciones, aunque estudios realizados estiman que puede afectar entre un 10-20% de individuos de distintos grupos etarios (Reyna 2018. pág. 191). Esta diferencia puede ser debido al miedo a denunciar, porque el ciberacoso es fácil de ocultar, el temor a no poder acceder al internet, a las redes sociales, a ser castigados por el agresor, la vergüenza de ser vistos como sujetos débiles este último en especialmente entre los niños y adolescentes (Ortega. 2012. págs. 38: 342-56).

b.- Grupo Etario

La relación entre edad y posibilidad de ser víctima de ciberacoso no es muy clara todavía ya que esta problemática puede ser experimentada por sujetos de diferentes edades, sin embargo, es más común entre los adolescentes, pero conforme la edad aumenta también crecer el número de individuos que son acosados. Estudios demuestran que los estudiantes son los más propensos al ciberacoso por el uso continuo de los equipos tecnológicos, especialmente el celular. (Reyna, 2018. pág. 192)

El género es considerado la característica más importante para el ciberacoso ya que fundamentalmente son las mujeres o las niñas las más propensas a ser las víctimas en tanto que el agresor es generalmente el hombre. Se sabe que la mujer tiene más posibilidades de ser el objeto de violencia cibernética a través del uso del correo electrónico, puesto que son más inclinadas a enviar o leer correos electrónicos, en tanto que los hombres realizan otro tipo de actividades en línea. (RPC, 2018. pág. 7)

Tampoco se descarta la posibilidad de que las mujeres efectúen ciberacoso, el ciberespacio les sirve para ocultarse pues al ser la acosadora (mujeres o niñas) se muestran débiles frente a sus víctimas al intentar asustarlas. (Reyna, 2018, pag. 192)

c.- Edad

Distintos estudios efectuados manifiestan que los jóvenes comprendidos entre 16 y 30 años son aquellos que están más expuestos al ciberacoso (Burgess y Baker, 2008. págs. 554-555) basados en que este grupo utiliza mucho más frecuentemente los contenidos y servicios que se ofrecen a través de los medios tecnológicos y que son utilizados como herramientas de ciberacoso. Es conocido también que los jóvenes utilizan en mayor proporción los PC fijos, tabletas, portátiles y teléfonos móviles para mantenerse conectados a internet a diferencia de los sujetos de otras edades; así también son los que menos utilizan sistemas de protección como son los antivirus que impedirían el acceso a sus claves personales o la suplantación de la identidad.

d.- Factores Psico-Sociales

Los agresores cibernéticos por lo general presentan alteración en su conducta psicosocial como: niveles bajos de conducta social, alta agresión tanto proactiva y reactiva, menor empatía y agresión elevada con relación a su entorno, son hiperactivos, utilizan sustancias ilícitas, conductas antisociales, problemas de concentración y falta de apoyo social entre otras, este último considerado muy significativo. (Torre-Montilla, 2018, pág. 193).

Es importante considerar también que los acosadores son propensos a ser acosados por lo tanto se convierten en víctima y agresor pues no existe vínculo emocional con la familia o amigos y siempre se agrupan con grupos de delincuentes. (Avilés, 2013, pág. 96).

Favorecidos por las nuevas tecnologías los ciberacosadores como vemos presentan diversos trastornos de conducta social con las cuales buscan satisfacer sus propios intereses y conseguir lo que desean sin importar el daño que causen a su víctima. Al hacer uso del poder objeto de estas conducta el ciberacosador buscan agruparse con delincuentes puesto lo que hace que socialmente se convierta en un personas peligrosa para la sociedad.

e.- Tecnologías usadas en el Ciberacoso

La tecnología para llevar a cabo el ciberacoso varia tanto en frecuencia como en el efecto que produce, a menudo la víctima avizora que la violencia cibernética es tan impactante como la tradicional o “cara a cara”. Sin embargo, en este tipo de violencia el uso de las imágenes, del video, el texto, el audio al distribuirse extensamente en la red se vuelve difícil de eliminar produciendo graves efectos emocionales en las victimas a lo largo de su vida (Torre-Montilla, 2018, pág. 193).

En nuestro país al respecto del uso de las tecnologías en el año 2002 se expide la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, con el fin de “impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos, así como contar con un instrumento legal que permita el uso de los servicios electrónicos incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales”. Tienen como objetivo “regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas”. (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, págs. 1-17).

En el artículo 9 de esta ley sobre la protección de datos expresa que:

> Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria

no tendrá en ningún caso efecto retroactivo. (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, págs.. 1-17).

Art. 10.- Procedencia e identidad de un mensaje de datos.- Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguiente casos: a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y, b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado. (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, págs. 1-17).

La presente ley en los artículos 9 y 10 manifiesta que para la transferencia de datos se requiere el consentimiento expreso del titular, el cual podrá elegir qué documento desea compartir, a terceros autoriza el uso de esos datos personales, además señala que se debe conocer cuál es el origen de los mensajes de datos y quien es la persona que lo emitió para verificar y tomar medidas en contra de la persona que lo ejecuto, esta protección de datos son garantizados tanto por la Constitución Política de la República y esta ley.

Hay que mencionar también que en esta Ley en la disposición general novena define a los mensajes de datos como “toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.” (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, pág. 15).

El 26 de mayo de 2021 se la Asamblea Nacional aprueba la Ley Orgánica de Protección de Datos Personales cuyo objetivo y finalidad citados en el artículo 1 es:

> Garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.
> (Ley Orgánica de Protección de Datos Personales, 2021, pág. 9)

El Artículo 8 respecto del consentimiento manifiesta que:

> Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea:
>
> 1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento;
>
> 2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento;
>
> 3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia,
>
> 4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular.
>
> El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento.
>
> El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos.
>
> Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado dará una pluralidad de finalidades será

> preciso que conste que dicho consentimiento se otorga para todas ellas. (Ley Orgánica de Protección de Datos Personales, 2021, pág. 15)

Es importante hacer hincapié de esta ley citar del Capítulo II tres principios que guardan relación con la protección de datos:

> b) Lealtad.- El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados.
>
> En ningún caso los datos personales podrán ser tratados a través de medios o para fines, ilícitos o desleales.
>
> c) Transparencia.- El tratamiento de casos personales deberá ser transparente. Por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro.
>
> Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su
>
> reglamento y demás normativa atinente a la materia.
>
> g) Confidencialidad.- El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley.
>
> Para tal efecto, el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio.

Esta ley como se puede observar instituye una autoridad de control para vigilar el cumplimiento de la normativa, especialmente, aquellas personas que llevan a cabo procesos de para el tratamiento de los datos personales, además, garantiza ejercicio de los derechos en protección de los de los ciudadanos.

La Constitución de la República en el artículo 3 de la Constitución de la República determina como deber primordial del Estado garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales; el artículo 16 ibídem dispone que todas las personas, en forma individual o colectiva, tienen derecho a la comunicación e información;

El artículo 66, numeral 19, ibídem reconoce y garantizará a las personas: “El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley” y en su numeral 21 garantiza a las personas “el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación” (Constitución de la República del Ecuador, 2008, págs. 16,47)

Con el fin de dar cumplimiento a lo establecido en a constitución y las leyes conexas en el año 2021 el gobierno nacional pública mediante Acuerdo Ministerial 006-2021 las Políticas de Ciberseguridad cuyo objetivo de conformidad con el artículo 1 es:

> Construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio.
>
> La política establece directrices que buscan afianzar un ciberespacio seguro para contribuir al desarrollo social, económico y humano del país, así como a la creación de una confianza digital que favorece el intercambio de información y, en consecuencia, de bienes y servicios en línea.

> La política tiene un enfoque multisectorial y multidimensional que se debe al carácter transversal de la ciberseguridad. Por tanto, la política alcanza a varios sectores y actores, públicos y privados, del país, y de manera vertical y horizontal. En esta medida, la política establece directrices para encaminar las acciones de las entidades de la Administración Pública Institucional y que dependen de la Función Ejecutiva, en coordinación con los otros poderes del Estado, sociedad civil y ciudadanía en general. (Ministerio de Telecomunicaciones y Sociedad de la información, Acuerdo Ministerial 006-2021, pág. 4)

> Los principios que rigen esta política son la promoción y el respeto de los derechos humanos y libertades fundamentales, el fomento de la confianza, la resiliencia, la responsabilidad compartida, el fomento del desarrollo de actividades en el entorno digital y el mercado nacional de TIC. En el marco de un Internet libre, abierto y seguro, prima la comunicación de las personas, la protección de datos, el derecho a la privacidad, y el marco de los objetivos de desarrollo sostenible. Esta política se basa en siete pilares que contemplan diversas temáticas de intervención del Estado, en coordinación con el sector privado, la academia y sociedad civil, que permitirán la ciberseguridad del Ecuador. (Políticas de Ciberseguridad, 2021, pág. 9)

Como lo manifiestas Michelena (2021), “Las políticas tienen alcance nacional, se alinean con la normativa y demás instrumentos de política pública. Debido al carácter ubicuo de la ciberseguridad, la política también se aplica al espectro radioeléctrico y en las infraestructuras digitales, donde se incluyen: los dominios, plataformas y programas donde se maneje información de carácter pública y privada de la población” (Michelena, 2021, pág. 9)

Las facilidades que prestan hoy en día el internet para conectarse y las aplicaciones creadas han promovido el aumento de los ciberdelitos entre los cuales podemos ver las estafas, la piratería, la usurpación de identidad, la pornografía infantil, entre otras, lo que lleva a la población a estar en peligro constante por ello en el país se ha implementado políticas de seguridad con el objeto de proteger la información, garantizar la integridad y confidencialidad.

Hay que recalcar que en estas políticas al hablar de los ciberdelitos al no estar tipificado el ciberacoso, poco o casi nada se hace al respecto.

f.- Características demográficas

No existen muchos estudios sobre las características demográficas de agresores y victimas en caso de violencia cibernética, tampoco sobre etnia o raza, región geográfica, tipo de educación, publica, privada, religiosidad entre otras; por otra parte, estudios revelan que hay una gran cantidad de víctimas de ciberacoso entre en homosexuales, lesbianas, bisexuales y transexuales, los individuos de razas diferentes a la blanca y los no heterosexuales experimentan ciberacoso de manera exagerada. (Torre-Montilla, 2018, pág. 193).

1.3. CARACTERÍSTICAS DIGITALES DEL CIBERACOSO

A más de las características anotadas anteriormente, Guzmán 2011 cita las siguientes características digitales: (a) Falsa acusación: La generalidad de los acosadores intentan dañar la reputación de la víctima manejando a gente contra él. (b) Publican información falsa sobre las víctimas en sitios web. Pueden crear sus propias webs, páginas de redes sociales (páginas de Facebook), blogs o fotologs para este propósito. Mientras el foro donde se aloja no sea eliminado, puede perpetuar el acoso durante meses o años. Y aunque se elimine la web, todo lo que se publica en Internet se queda en la red. (c) Recopilación de información sobre la víctima: Los ciberacosadores espían a los amigos de la víctima, su familia y compañeros de trabajo para obtener información personal. (d) Monitorizarán las actividades de la víctima e intentarán rastrear su dirección de IP en un intento de obtener más información sobre ésta. (e) Envían de forma periódica correos difamatorios al entorno de la víctima para manipularlos. (f) Manipulan a otros para que acosen a la víctima. La mayoría tratan de implicar a terceros quienes toman fotos o vídeos comprometedores. A menudo la víctima desconoce la existencia de estos hechos, debido al silencio de los testigos. (g) El acoso se hace público, el acosador traslada a Internet sus insultos y amenazas haciendo pública la identidad de la víctima en un foro determinado (blogs,

websites), redes sociales incluso facilitando en algunos casos sus teléfonos, de manera que gente extraña se puede adherir a la agresión. (h) Ataques sobre datos y equipos informáticos, tratan de dañar el ordenador de la víctima enviando virus. (i) Desamparo legal de estas formas de acoso, ya que, aunque cierren una Web con contenido sobre la víctima, puede abrirse otra inmediatamente. (j)

El acoso invade ámbitos de privacidad y aparente seguridad como es el hogar familiar, desarrollando el sentimiento de desprotección total. (k) No necesaria la proximidad física con la víctima. El 'ciberacoso' se puede perpetrar en cualquier lugar y momento sin necesidad de que el acosador y la víctima coincidan ni en el espacio ni en el tiempo. (Guzmán, 2011, párr. 6)

Acerca de las características enunciadas por Guzmán respecto del ciberacoso manifiesta entre otras que el ciberacosador al tener amplios conocimientos y destrezas para acceder al internet le facilita llevar a cabo conductas delictivas como sustraerse información privada, crean perfiles falsos de las víctimas, invadir la privacidad, realizan publicaciones con el propósito de intimidarla, entre otras aprovechando que no existe normativa legal que se lo impida por lo tanto tiene un espacio abierto para seguir con sus conductas delictivas.

1.4 FACTORES DE RIESGO EN EL CIBERACOSO

A pesar de que no existen investigaciones profundas o exhaustivas sobre los factores de riesgos en el ciberacoso o la violencia cibernética, si existen datos estadísticos que dan cuenta del alto porcentaje de individuos que desde los 10 años utilizan ordenadores, celulares, tabletas, así como del uso de internet y de las redes sociales hasta en un 100% lo cual da cuenta que la sociedad actual se encuentra hiperconectada sin tener en cuenta edad.

El uso de internet y de medios tecnológicos al incrementarse en los últimos año y al existir pocos mecanismo de control frente al manejo del tiempo que se emplea frente a un computador, teléfono móvil, tabletas, entre otros y el uso de la información que se produce en la red se pueden observar numerosos riesgos a los que se está expuestos lo cibernautas como la difusión instantánea de la información que se comparte en las redes, el número de personas con

identidad anónima con las cuales se entra en contacto y el contenido que se descarga y se sube en las redes como lo manifiesta (Cross et al., 2015 citado en Hennning et al. 2019, pág. 7).

Igualmente de los escasos estudios realizados en materia de ciberacoso estos reportan que las víctimas exhiben factores de riesgo relacionados en el ámbito psicológico e individual como justificar a los ciberacosadores por sus conductas y sentirse culpable. En relación al sexo, el factor de riesgo se da tanto en hombre como en mujeres. Se advierte además baja autoestima y empatía, sentir ira y frustración, tener historial de problemas de salud mental, percepción de baja autoeficacia y bajos niveles de estima corporal. En cuanto a los factores de riesgo relacionados con los ciber agresores se ha encontrado que encontrado que pertenecen principalmente al género masculino, la desvinculación moral frente a la situación de la víctima, falsear las consecuencias de sus propias conductas, culpar a las víctimas por su actuación, ajos niveles de autoestima, baja empatía, así como altos niveles de agresividad. (Marín-Cortés, et.al, 2019, pág. 111).

La oficina de las Naciones Unidas para la Reducción del Riesgo de Desastres define al riesgo como la combinación de la amenaza, la vulnerabilidad, la violencia, y las capacidades de un sujeto o persona y el riesgo se mide en términos de impacto y probabilidad. De esta definición vemos entonces que hay más probabilidad que mediante la elaboración de un acto sea posible que se reduzca la capacidad de un individuo para actuar frente a un riesgo definido.

Indiscutiblemente las personas que usan generalmente las redes sociales, computadoras software de mensajería instantánea, por un periodo prologando de tiempo, ya sea con poco o nulo conocimiento en tecnología son personas vulnerables ya que permiten la publicación de fotografías, videos, o información personal en sus redes sociales entre otras. A continuación, detallaremos los principales riesgos del ciberacoso.

a.- Uso de Internet y TIC

Las víctimas de ciberacoso por lo general hacen uso del internet por más de tres horas incluso si no tienen habilidades para ello mediante de la utilización de

computadores, teléfonos inteligentes, redes sociales e incluso los software de mensajería instantánea, permiten que otros individuos coloquen en la red sus videos y fotografías personales, son sujetos de acoso cibernético a muy temprana edad, tienen un alto conocimiento del anonimato que ofrece la Web, suelen acceder a Internet desde distintos sitios como por ejemplo un café, son usuario frecuentes de videojuegos online, divulgan información personal y buscan apoyo e interrelación permanente a través de las redes sociales. (Marín-Cortés, et.al, 2019, pág. 111)

b.- Aspectos familiares y sociales

En las víctimas de violencia cibernética se encontraron diversos factores de riesgo como es el caso de haber sufrido antes de bullying o acoso tradicional ”que es la agresión para ejercer poder sobre otra persona a través una serie de amenazas hostiles, físicas o verbales que se repiten, angustiando a la víctima y estableciendo un desequilibrio de poder entre ella y su acosador” (UNICEF. 2018), frecuente ausentismo escolar, supervisión habitual en el uso de tecnologías digitales por sus padres, escaso o ningún tipo de apoyo social y sentimientos de soledad,

Para ser parte de una minoría étnica, mostrar problemas de comunicación con los padres, autoritarismo paterno, historial de abuso sexual en la infancia. En cuanto al acosador se destaca su poca vinculación con sus maestros, faltas permanentes a su lugar de estudio, la idea de tener poca compañía, presión social de otros ciber agresores, estilo paternal autoritario, bajo involucramiento de sus progenitores como por ejemplo en las tareas escolares de sus hijos, manifestar comportamientos violentos, participar en actos delincuenciales y el consumo de sustancias ilegales o alcohol. (Marín-Cortés, et.al, 2019, pág. 111)

b.1 Aspectos familiares

Las investigaciones realizadas respecto de cuál es la influencia familiar en el ciberacoso han dado como resultados que tanto víctimas como agresores son propensos a estilos de crianza negativos. Los conflictos al interno de la familia se relacionan con comportamientos intimidatorios ya que los menores al ser testigos de la violencia entre sus padres son más proclives a intimidar a sus pares. La sobreprotección de sus padres, dificultan el desarrollo de su

autonomía y su interacción social, lo que vuelve a los hijos e hijas vulnerables a ser víctimas de acoso por sus iguales, como consecuencia de la baja habilidad para afrontar la solución de conflictos.

Por otra parte si el individuo no percibe apoyo de otras personas importantes en su entorno se asocia negativamente con la perpetración del ciberacoso, aquellos que mantienen vínculos emocionales más débiles con sus padres no se llevan bien con ellos, no tienen demasiada confianza, no comparten sus problemas y no realizan actividades juntos y que mantiene poca vigilancia de sus padres de sus actividades en internet y las redes tienen una mayor probabilidad de convertirse en ciberacosadores. Los investigadores han identificado una relación negativa entre el control de la tecnología por parte de los padres y la cibervictimización así a mayor control menor victimización,, los estudio también han revelado que si los padres mantiene una buena comunicación y se platica con los hijos sobre la conducta que den tener al usar el internet existe una menor cibervictimización. (Sánchez, 2016, pag. 30-31).

En general, se puede manifestar que el clima familiar donde exista apoyo, respeto, calidez, normas claras, buena comunicación, son ambientes óptimos para la protección contra el ciberacoso o cyberbullying. Por otra lado si existe estilos autoritarios donde se encuentre un exagerado nivel de normas y bajo afecto, demasiada permisividad, violencia familia, falta de apoyo, poca o ninguna comunicación entre otras causas ya anotadas se relacionan con la victimización y la agresión en el cyberbullying.

b.2 Aspectos sociales

El uso intensivo de la red, la penetración de los smartphones y la penetración de las redes sociales ha dado lugar a la aparición del ciberacoso y maltrato psicológico través de las TIC, debido al anonimato que tiene sus usuarios.

De acuerdo con Madrid, et. al (2020) El ciberacoso afecta de forma negativa el desarrollo psicosocial de los involucrados directa o indirectamente en el mismo. En las cibervíctimas, como ejemplo se observa disminución del desempeño académico, estrés, depresión, baja satisfacción con la vida e ideas suicidas.. La investigación sugiere también la influencia de la comunidad en el ajuste social de los individuos, mientras que indicadores de desorganización abuso de drogas,

criminalidad, carencias estructurales y exposición a la violencia provocan prevalencia de conductas agresivas. Si bien la evidencia disponible sugiere que las características del contexto social influyen en el desarrollo de los individuos, se han encontrado pocos estudios que relacionen las características de la comunidad con el ciberacoso. En estas investigaciones se asocia el ciberacoso con amistades antisociales la exposición a situaciones de violencia y el bajo compromiso con la comunidad. (Madrid, et .al, 2020, párr. 10)

Concluyendo podemos decir que los individuos que cuenta con más apoyo social se implican menos con ciberagresores, mientras quienes tienen menor apoyo más propensos a ser víctimas del ciberacoso.

c.- Aspectos psicológicos e individuales

Las cibervíctimas en cuanto a aspectos psicológicos e individuales presentan: favorabilidad frente al acosador, alta justificación a los ciber acosadores, considerarse culpable, con relación al sexo es un alto factor de riesgo tanto en hombres como en mujeres. Se observa además una baja autoestima y empatía, bajo nivel escolar respecto del agresor, presentan crisis de ira y frustración, suelen tener un largo historial de problemas de salud mental, baja autoeficacia y bajos niveles de estima corporal. En relación con los ciberagresores estos presentan frialdad moral frente a la situación de la víctima, tergiversar las consecuencias de sus propias conductas, culpar a las víctimas por su situación, bajos niveles de autoestima, baja empatía, déficit en la comunicación emocional así también altos niveles de agresividad. (Marín-Cortés, et.al, 2019, pág. 112),

d.- Riesgo de Privacidad

A través del uso de redes sociales, mensajería o cualquier otro tipo de software de comunicación que unas personas utiliza, se convierte en un factor de riesgo muy alto ya que el ciberacosador hace unos de los datos personales para invadir la privacidad, la intimidad, enviar mensaje no deseados a su víctima e incluso a su círculo personal.

e.- Riesgos de Contacto

Por medio de los chats las personas se pueden contactar con otras personas, pero cuyos fines sean malévolos, por ejemplo, en el Grooming que “es la acción deliberada de un adulto, varón o mujer, de acosar sexualmente a una niña, niño o adolescente a través de un medio digital” (Escobar, 2015), utilizando la mentira para hacerse pasar como amigos de su edad.

Entre los riesgos de violencia cibernética en este ámbito se pueden presentar las siguientes: subir una foto montada que sea real y vergonzosa para la víctima, crear un espacio con el nombre del acosado, emitir rumores sobre una actitud reprochable e incluso poner videos donde se insulta a la víctima.

1.5 PROTAGONISTAS DEL CIBERACOSO

De acuerdo con Sánchez Pardo y colaboradores (2016, pag. 21) existen tres protagonistas que intervienen en el ciberacoso: los agresores o agresoras, las víctimas y los testigos.

a.- El agresor

Para López (2012) citado en Granizo, 2018. Pág. 37. un acosador es un depredador que puede esperar pacientemente conectado a la red, participar en chat o en foros hasta que entabla contacto con alguien que le parece susceptible de molestar, generalmente mujeres o niños; y que disfruta persiguiendo a una persona determinada, ya tenga relación directa con ella o sea una completa desconocida. El acosador disfruta y muestra su poder persiguiendo y dañando psicológicamente a esa persona. (López, 2012 pag.)

El ciberacosador se siente en una posición de poder desde el anonimato que se percibe mientras se está “en línea”. Durante todo ese tiempo va recopilando toda la información posible acerca de su víctima, fundamentalmente en aquellos aspectos que forman parte de su vida privada y de sus movimientos en la Red. Una vez obtenida dicha información, es cuando el acosador inicia su proceso de acoso. En el caso de ciberacoso, se añade la característica de cobarde, ya que se oculta tras el aparente anonimato y falsificación de identidad que proporciona internet”

El acosador es un sujeto muy hábil para infringir temor, su carácter y rudeza hace que las personas lo idealicen. Con respecto a sus características el acosador tiene una inadecuada composición social, conflictos afectivos, escasa empatía, trastornos de personalidad, incapacidad para sentir emociones, déficit de atención, falta de respeto hacia los demás y una muy importante son considerados como los más populares.

Entre las causas que llevan a los sujetos a actuar como acosadores están la irá, envidia, venganza, falta de madurez, fastidio, reproducción de conductas, demostración de poder, discriminación racial o sexual, entre otras, sin embargo en algunos casos va más allá de estos factores, como actuar precipitadamente por sus emociones negativas ante ciertas conductas personales, y en otros casos se puede participar en ciber acoso por el simple hecho de exponer su habilidad tecnológica ya sea por diversión o la sensación de sentirse poderoso frente a otras personas. (Sánchez 2016, pag.30-31)

Según Sullivan, et.al, (2010. Pag. 116) los tipos de acosadores son:
a.1 Acosador Inteligente

a.2 Acosador Poco Inteligente

a.3 Acosador Víctima

b.- La víctima

Castells (2007) manifiesta que esta persona es incapaz de defenderse y siempre la excluyen de cualquier tipo de actividad, por lo que esta reacción hace que la víctima sea solitaria y propensa a recibir cualquier tipo de acoso por parte del agresor, su situación de desamparo y frente a un mecanismo donde el maltrato y dominio crece hace que su lucha sea inútil al momento de verificar un estado. (Castell. 2007, págs. 27-179)

Para Harris y Petrie (2006), los perfiles de las víctimas son determinados por la intimidación; ya sea dentro de su contextura corporal, el tener rasgos físicos distintos a los demás, poseer algún tipo de discapacidad, ya sea utilizar lentes,

ser obeso o simplemente pertenecer a un nivel social sean estos etnia, raza o religión. Su identidad, contextura física, rasgos faciales, personalidad, vestimenta conforman un conjunto de herramientas que configuren la epidemia del acoso cibernético. (Harris, S., & Petrie, 2006. Págs. 58- 59)

De acuerdo con Avilés (2005, pag. 27-41) Los tipos de víctimas se clasifican en:
b.1 Victima Activa

b.2 Victima Pasiva

Por su parte Carrasco y Navas (2013, págs. 3-4) mencionan que existen dos tipos de víctimas

b.3 Víctimas pasivas

b.4 Víctimas provocadoras acosadores-víctimas

c.- El espectador

Es un individuo que no interviene directamente ni con el agresor ni con ni la víctima, es un simple espectador o testigo, que contribuye de manera indirecta toda vez que es el que visualiza y tiene conocimiento de situaciones de ciberacoso. El espectador es la persona que no tiene mayor interacción con las conductas de acoso sin embargo estas conductas no se darían si el testigo brindara ayuda oportuna a la víctima dando a conocer sobre los hechos sucedidos para que no se vuelvan a repetir. (Sullivan, 2010. Pag. 116.)

Por otro lado, los testigos suelen incentivar al acosador de forma directa o indirecta por ejemplo de manera directa al participar en las redes sociales comentando o reaccionando a los comentarios del agresor y de forma indirecta mostrando indiferencia sobre los actos del agresor. Algunos estudios señalan que los espectadores digitales son más propensos a participar activamente en el acoso cibernético mediante el envío de fotos de la víctima que en actos de intimidación que tienen lugar cara a cara. (Marín-Cortez. 2019 pag. 112)

Otro aspecto importante para considerar es que este tipo de sujetos tiende a deshumanizar a la víctima e ignoran e ignoran las consecuencias, frecuentemente renuncian a toda responsabilidad y muchas veces son quienes

gozan de la agresión, pero tiene sentimientos de culpa por el hecho suscitado. Como manifiesta Sullivan (2005, Pag. 116) es posible que ellos también sufran de alguna clase de intimidación y no denuncian el por miedo a ser también víctima del acosador, por ello carga con el peso de ser amigo de la víctima e intenta cambiar su accionar dentro del proceso de la intimidación y asume asumiendo roles como:

Compinches: Son amigos íntimos del acosador, es decir; que forman parte del grupo social de la persona activa de este terrible acoso.

Reforzadores: Actúan en cierto modo con su apoya a la intimidación.

Ajenos: Intentan no llamar la atención su apariencia es neutral y pueden tolerar la intimidación y ser inmunes a ella.

Defensores: Son los que muestran el coraje de abandonar su papel de encubridores.

CAPITULO II: EL INTERNET Y LAS REDES SOCIALES

En el presente capítulo versará sobre el internet y las redes social, iniciando con una definición de internet, seguidamente se realiza una breve historia de este para continuar con la redes sociales, igualmente se define que es una red social, su historia, característica, tipos de redes y el uso de las mismas**.**

2.1 EL INTERNET

Se puede definir al Internet como un conjunto de ordenadores interconectados globalmente, a través de los cuales todo el mundo puede acceder de manera rápida a datos y programas desde cualquier lugar. Es también una herramienta de difusión mundial, un conjunto de mecanismos para propagar información y un medio para que las persona interactúen y colaboren entre si y sus ordenadores sin considerar su ubicación geográfica.

2.2 BREVE HISTORIA DE INTERNET

Antes de crearse el Internet o la llamada red de redes, la única manera que el ser humano tenía para comunicarse de forma digital era el telégrafo. El telégrafo se inventó en 1840, teniendo como característica emitir señales eléctricas que viajaban por cables enlazados desde un origen hacia un destino, para interpretar la información que era enviada se utilizaba el código Morse.

En 1958 los EE. UU., fundaron la Advanced Researchs Projects Agency (ARPA) a través del Ministerio de Defensa. El ARPA se centró en crear comunicaciones directas entre ordenadores para poder comunicar las diferentes bases de investigación. En 1962, el ARPA creó un programa de investigación computacional bajo la dirección de John Licklider, un científico del MIT (Massachusetts Institute of Technology). En 1967 ya se había hecho suficiente trabajo para que el ARPA publicara un plan para crear una red de ordenadores denominada ARPANET. ARPANET recopilaba las mejores idas de los equipos

del MIT, el National Physics Laboratory (UK) y la Rand Corporation. La red fue creciendo y en 1971 ARPANET tenía 23 puntos conectados. (FIB 2018)

En 1972 ARPANET se presentó en la First International Conference on Computers and Communication en Washington DC. Los científicos de ARPANET demostraron que el sistema era operativo creando una red de 40 puntos conectados en diferentes localizaciones. Esto estimuló la búsqueda en este campo y se crearon otras redes. Entre 1974 y 1982 se crearon gran cantidad de redes. En 1982, ARPANET adoptó el protocolo TCP/IP y en aquel momento se creó Internet (International Net). (FIB 2018)

A principios de los 80 se comenzaron a desarrollar los ordenadores de forma exponencial. EL crecimiento era tan veloz que se temía que las redes se bloquearan debido al gran número de usuarios y de información transmitida, hecho causado por el fenómeno e-mail. La red siguió creciendo exponencialmente (FIB 2018.)

El World Wide Web (WWW) es una red de “sitios” que pueden ser buscados y mostrados con un protocolo llamado HyperText Transfer Protocol (HTTP) fue diseñado por Tim Berners-Lee y algunos científicos del CERN (Conseil Européen pour la Recherche Nucléaire) en Ginebra. Estos científicos estaban muy interesados en poder buscar y mostrar fácilmente documentación a través de Internet. Los científicos del CERN diseñaron un navegador/editor y le pusieron el nombre de World Wide Web. (FIB 2018)

En 1991 esta tecnología fue presentada al público a pesar de que el crecimiento en su utilización no fue muy espectacular, a finales de 1992 solamente había 50 sitios web en el mundo, y en 1993 había 150. En 1993 Mark Andreesen, del National Center for SuperComputing Applications (NCSA) de Illinois publicó el Mosaic X, un navegador fácil de instalar y de usar. A partir de la publicación de la tecnología WWW y de los navegadores se comenzó a abrir Internet a un público más amplio: actividades comerciales, páginas personales, etc. Este crecimiento se aceleró con la aparición de nuevos ordenadores más baratos y potentes (FIB 2018).

Actualmente el Internet ofrece el correo electrónico o e-mail, permite escribir, guardar, enviar y recibir correo mediante sistemas de comunicación electrónicos. El correo electrónico ha revolucionado las comunicaciones entre las personas. Los chats que ofrecen la posibilidad de comunicarse entre muchas persones por escrito a través de Internet. Los chats han permitido a las personas que los usan la comunicación con otros usuarios de manera anónima (FIB 2018).

Como se pude evidenciar desde la creación del internet en los años 80, éste ha ido evolucionando significativamente, anteriormente solo se podía comunicar con una persona de forma digital a través del telégrafo, en la actualidad el internet ofrece varios mecanismos de comunicación, la rapidez y facilidad esto ha llevado a que los usuarios de este medio accedan a través de la redes sociales, chats, mensajes de correo, para comunicarse con otras personas de una manera muy sencillas y rápidas, sin embargo este avance del internet a traído problemas por cuanto los usuarios utilizan en anonimato para causar daño a los cibernautas.

2.3 LAS REDES SOCIALES

Hoy en día las redes sociales en Internet han ganado su lugar de una manera vertiginosa convirtiéndose en promisorios negocios para empresas y sobre todo en lugares para encuentros humanos. Para comprender un poco este fenómeno en crecimiento presuroso cabe citar en principio alguna definición básica que nos permita comprender que es una red social, cómo funcionan en Internet y algunas nociones sobre su historia.

De acuerdo con la ponencia presentada en las Jornadas sobre Gestión en Organizaciones del Tercer Sector en la Universidad Di Tella de Buenos Aires, Argentina, en noviembre de 2001, las redes son formas de interacción social, definida como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos. Una sociedad fragmentada en minorías aisladas, discriminadas, que ha desvitalizado sus redes vinculares, con ciudadanos carentes de protagonismo en procesos

transformadores, se condena a una democracia restringida. La intervención en red es un intento reflexivo y organizador de esas interacciones e intercambios, donde el sujeto se funda a sí mismo diferenciándose de otros.

Las redes sociales en Internet permiten la posibilidad de interactuar con otras personas, aunque no se las conozca ya que el sistema es abierto y se va construyendo con lo que cada suscriptor de la red aporta. Cada uno de los nuevos miembros que ingresa a las redes convierte al grupo en otro nuevo. Al ser parte de una red social los sujetos comienzan buscando a otros con quienes compartir intereses, preocupaciones o necesidades lo cual permite romper el aislamiento a la gran mayoría de las personas. Las redes sociales también proporcionan al anonimato popularidad, al discriminado lo integran, a la diferente igualdad y así muchos otros aspectos. La fuerza del grupo permite sobre el individuo cambios que de otra manera podrían ser difíciles y genera nuevos vínculos afectivos, de negocios e incluso hoy en día del llamado acoso cibernético (Pazmiño 2010).

2.4 HISTORIA DE LA REDES SOCIALES

Alrededor de 2001 y 2002 surgen los primeros sitios que fomentan redes de amigos. Hacia 2003 se hacen populares con la aparición de sitios tales como Friendster, Tribe y MySpace. Rápidamente algunas empresas ingresan a las redes sociales. Google lanza en enero de 2004 Orkut apoyando un experimento que uno de sus empleados realizaba en su tiempo libre. En 2005 ingresan Yahoo! 360º y otros. Básicamente el funcionamiento comienza cuando una vez montado el soporte técnico, un grupo de iniciadores invitan a amigos y conocidos a formar parte de la red social, cada miembro nuevo puede traer consigo muchos nuevos miembros y el crecimiento de esa red social puede ser geométrico. Y he aquí que se transforma en un interesante negocio. Un ejemplo de esto es Facebook, una red social enfocada a todas las edades, muy similar a MySpace, con millones de usuarios registrados y donde ha habido una importante inversión publicitaria de parte de Microsoft (Gonzáles, 2009, párr.. 2-3).

2.5 CARACTERÍSTICAS DE LAS REDES SOCIALES

Como ya se dijo anteriormente, las redes sociales son sitios de internet que permiten a los usuarios compartir y publicar información, comunicarse con otras personas y crear grandes comunidades. Esta herramienta que tiene como objetivo la comunicación sencilla y eficiente entre grupos de interés, también facilita las relaciones sociales y la proyección de empresas y servicios y hoy en día se ha convertido en un medio para delinquir, acosar, intimidar, invadir la privacidad, entre otras.

Las redes sociales, presentan las siguientes características:

a.- Conectividad

Las redes sociales conceden a los usuarios facilidades para conectarse con otros usuarios con los cuales pueden compartir comparten particularidades y satisfacer la necesidad de pertenecer a un grupo o comunidad.

La forma en que están diseñadas las redes sociales muestran las técnicas para que entre las personas se den vínculos, aunque este vínculo sea más frágil que aquellos que son creados en la vida cotidiana. Las redes sociales han favorecido tener cercanía con personas de diferentes países, pero con intereses comunes; por este medio los usuarios pueden seguir a otros usuarios o ser seguidos, permitiendo más personas estén interconectadas.

b.- Gratuidad

Las redes sociales mayoritariamente son gratuitas, ya que sus ingresos los obtiene a través de la publicidad exceptuando aquellas redes sociales privadas.

Dada la gran cantidad de usuarios de las redes sociales, estas se convierten en un medio para la publicidad y atraer a posibles consumidores de forma rápida, por esta característica, las redes sociales se han convertido en un medio de publicidad de bajo costo, pero con gran efectividad, en relación a otros medios de comunicación como la radio, televisión o el periódico.

c.- Instantáneo

Los mensajes y publicaciones en las redes sociales son creados de manera instantánea, permitiendo que la información esté actualizada permanentemente y los usuarios se comuniquen entre ellos de forma rápida y eficaz. Varias de estas plataformas permiten notificaciones para que los usuarios se enteren rápidamente de los sucesos u acontecimientos del día a día.

En ocasiones al ser la información emitida de manera muy rápida da lugar al aparecimiento de noticias falsas o a la reproducción en mayor cantidad de hechos que no ha sido confirmado.

d.- Viralidad

Un contenido al ser difundido por el internet puede volverse viral y propagarse aceleradamente por medio de las diversas redes sociales, provocando un gran impacto y logrando un gran alcance. Los contenidos que se vuelven virales son capaces de agitar las emociones de las personas o usuarios de la red.

e.- Personalización

Los usuarios de estos medios pueden personalizar sus perfiles a su gusto, puesto que las redes sociales permiten modificar o ajustar sus componentes para bienestar y satisfacción del usuario. Mediante las publicaciones realizadas, los usuarios pueden dar a conocer sus ideas e iniciar conversaciones con otras personas. Actualmente, se utilizan las publicaciones también para mostrar inconformidad, alegría o aprobación ante temas de interés social, político, económico, así como también para intimidar, acosar, suplantar, entre otros.

A nivel empresarial estas aprovechan la gran cantidad de información para conocer la opinión de la gente, saber más a fondo los gustos o preferencias de los usuarios y así relacionarse mejor y ofrecer servicios de interés.

2.6 TIPOS DE REDES SOCIALES

Cuando pensamos en redes sociales rápidamente viene a nuestra mente Facebook, Twitter o Instagram, pero al investigar observamos que existen un

sinnúmero de redes sociales, sin embargo para este estudio se las ha reunido en dos grandes grupos (Navarrete, 2020, párr. 1)

a.- Redes Sociales Horizontales

Son aquellas redes sociales de índole general ya que cualquier usuario puede ingresar y participar en ellas además de no tener características comunes entre estas están Facebook, Instagram o Twitter.

b.- Redes Sociales Verticales

En este tipo de redes los usuarios buscan o mantienen información en común y sirven para uno o varias objetivos concretos especialmente de nivel profesional como buscar empleo, viajes, networking entre otras en este grupo podemos encontrar redes como: LinkedIn, Tripadvisor, Spotify, Vimeo entre otras más.

Tabla 1 Tipos de Redes Sociales

Según finalidad	Según modo de funcionamiento	Según grado de apertura	Según nivel de integración
De ocio	De contenidos	Públicas	De integración vertical
De uso profesional	Basada en perfiles: personales/profesionales	Privadas	De integración horizontal
	Microblogging		

Fuente: ONTSI
Recuperado de https://www.ontsi.es//sites/ontsi/files/redes_sociales-documento_0.pdf

2.7 INFLUENCIA DE LAS REDES SOCIALES

Las funcionalidades de cualquiera de estas redes varían de manera pues algunas permite colocar fotografías, videos, tener mensajería para el envío y

recepción de mensajes privados o públicos; buscar pareja, armar grupos, hacer amigos, crear negocios, compartir música entre otros, para lo cual actualmente se apoyan en los teléfonos móviles. También la redes debido a la situación de pandemia experimentadas por COVID 19 en 2020 han impulsado de forma agresiva el comercio electrónico a través de la creación de tiendas on-line desarrolladas por empresas y personas naturales (Ureña, 2011, pág. 82)

2.8 USO DE LAS REDES SOCIALES

a.- Uso positivo de las redes

Las redes sociales inicialmente se consideraron un medio para comunicarse, sin embargo con el avance de la tecnología hoy en día sirven para: (i) El entretenimiento pues son un medio para el ocio. (ii) Para obtener información inmediata.(iii) Es un medio para contactarse con otras personas o para buscarlas pueden ser estos familiares, amigos, conocidos, entre otros que pueden estar cerca o bien alejados geográficamente. (iv) En la actualidad es un medio eficaz para establecer contactos con profesionales. (v) Crear comunidades online sea en relación a una empresa o de manera personal. (vi) Para hacer publicidad online de un producto, un servicio o una marca. (Sierra del Valle, 2011, pág. 15)

b.- Uso negativo de las redes sociales

Hay que mencionar, además que de acuerdo con estudios realizados las redes sociales muestran un alto índice de usuarios que hacen uso excesivo de este medio de comunicación y conexión permanente debido a su atractivo.

El Comité Económico y Social Europeo (CESE), ha reconocido como aspectos negativos y de riesgo los siguientes: (i) Los riesgos psicológicos derivados de insultos transmitidos por esos medios. (ii) El acoso sexual a niños y jóvenes. (iii) La exhibición en formatos multimedia de adolescentes desnudos. (iv) Los anuncios de prostitución. (v) La violación de la privacidad, la honra y la dignidad

personal. (vi) Los atentados contra la salud física y mental de los usuarios. (Sierra del Valle, 2011, pág. 15)

Como se afirma en los dos párrafos anteriores, específicamente las redes sociales, tienen un gran atractivo, lo que hace que los usuarios le den excesivo uso, originando problemas y riesgos como: ser víctima de acoso generalmente en menores de edad ya que son los más vulnerables, la divulgación de contenido personal, daños psicológicos, acoso sexual, entre otros que a futuro serán perjudicaran a quienes son víctimas del uso de estas redes

2.9 REDES SOCIALES MÁS UTILIZADAS

Las redes sociales en la actualidad evidencian que son "poderosos canales de comunicación e interacción, que permiten a los usuarios actuar como grupos segmentados de: ocio, comunicación, profesionalización, entre otros, siendo uno de los principales objetivos de la red social el momento en el que sus miembros utilizan el medio online para convocar actos y acciones que tengan efectos en el mundo *offline*" (Gonzalez, 2010, párr.. 2-3).

A continuación de se describirán brevemente las redes sociales más utilizadas actualmente:

a.- Facebook

Es la red social más empleada en el mundo dada su facilidad de uso, a través de esta red es fácil interactuar con otros usuarios pues permite compartir textos, fotos y videos Esta red la utiliza toda la familia desde los más jóvenes hasta los adultos. Es una de las redes las más utilizadas pues permite transmisiones por disponer de herramientas de geolocalización y segmentación. Se considera que esta red tiene alrededor de 2.320 millones de usuarios en el mundo (Digital 2021 Global Overview Report).

b.- WhatsApp

Es considerado el gigante de la mensajería instantánea, es una aplicación para teléfonos inteligentes más utilizada pues a través de esta se puede enviar y recibir mensajes, fotos, mensajes de voz, vídeos, imágenes, links, entre otros.Actualmente mantiene alrededor de 1.600 millones de usuarios (Digital 2021 Global Overview Report).

c.- Youtube

Aunque es una plataforma de video, es una red social de las más utilizadas por su capacidad de interrelación, permite compartir todo tipo de videos: musicales, educativos, empresariales, publicidad entre otros. Esta red es muy popular debido al uso de los influencers o Youtubers y mantiene alrededor de 1.900 millones de usuarios (Digital 2021 Global Overview Report).

d.- Instagram

Instagram es la red que comparte videos y fotos de manera simple y llamativa para los usuarios, es muy utilizada por los más jóvenes y al momento es una plataforma que permite la promoción y difusión de productos o servicios, con alrededor 1.000 millones de usuarios (Digital 2021 Global Overview Report).

e.- TikTok

La red social TikTok es la red que crece constantemente, actualmente se encuentra con más de 800 millones de usuarios (Digital 2021 Global Overview Report). Esta aplicación permite crear y compartir vídeos cortos de toda índole.

f.- Twitter

Es una red que permite el intercambio de opiniones en temas de actualidad y tendencias, hoy por hoy esta red está en descenso debido a la alta tasa de abandono de usuarios que tiene (Digital 2021 Global Overview Report).

g.- LinkedIn

Esta red social lo que busca usuarios con perfiles de profesionales e intercambiar ofertas laborales.Actualmente tiene alrededor de 300 millones de usuarios (Digital 2021 Global Overview Report).

h.- Tinder

Tinder es una aplicación de citas, encuentros e incluso se le puede considerar como una red social. Con ella se puede chatear y conseguir una cita con personas con quienes existe gusto en común o entre quienes se han seleccionado mutuamente. (Tinder. 2022)

i.- Badoo

Es una de las aplicaciones más exitosas y se puede utilizar tanto desde el móvil como desde el ordenador para buscar gente. En mayo de 2012, la compañía anunció que había alcanzado los 150 millones de usuarios registrados en todo el mundo.

La seguridad en las redes hoy en día es un gran problema para las grandes empresas proveedoras de este servicio debido a los ataques de los cuales son objeto por ello lo que buscan hoy en día es brindar la suficiente garantía y confiabilidad para que los usuarios puedan bajo un clima de confianza navegar, sin embargo por el avance de la tecnología las políticas implementadas no ha dado buenos resultados ya que cada vez existe personas que ingresan fácilmente estos servicios con el afán de causar daño tanto a las empresas como a los individuos.

2.10 LAS REDES SOCIALES EN EL ECUADOR

El *Digital 2021 Global Overview Report* publicado por *We are Social y Hootsuite*, efectúa un análisis estadístico de la situación digital en nuestro país en el 2020 – 2021 como se aprecia a continuación:

> En este informe se expone el crecimiento que ha experimentado el país durante el año 2020 en relación al uso del Internet y las nuevas prácticas de consumo que han surgido debido a la pandemia de COVID-19.

El país tiene una población total de 17.77 millones de habitantes, de los cuales el 64,3% reside en zonas urbanas.

Actualmente 13.82 millones es el número de dispositivos móviles conectados lo que constituye un 77,8% de la población.

Existen 10.17 millones de usuarios de internet y 14 millones de perfiles de redes sociales, lo que representa el 78,8% de la población.

Según un reporte del diario El País; en el Ecuador solo el 16% de los hogares rurales posee internet y las señales gratuitas en lugares públicos han sido una solución para la brecha digital en el país

Gráfico 1 Uso de internet, móviles y redes sociales

suite

Recuperado de: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-ecuador-en-el-2020-2021/

De acuerdo con el informe indicado, el auge de las plataformas digitales de comunicación instantánea y redes sociales durante la pandemia ha llevado a la mayoría de los ecuatorianos a estar conectados para enviar, revisar y compartir información de toda índole (We are Social y Hootsuite, 2020).

En Ecuador se mantienen activos 14 millones de perfiles en las redes sociales, es decir, el 78,8% de la población, existiendo un incremento de 2 millones de usuarios en comparación con el año anterior. Del total de usuarios que utilizan

las redes sociales el 98% acceden a través de sus dispositivos móviles (We are Social y Hootsuite, 2020).

Según datos del informe Ecuador Estado Digital 2021; Facebook, Instagram, TikTok y Twitter son las más populares en Ecuador, siendo Facebook la red social más visitada en navegadores web.

Finalmente, el estudio reporta que un ecuatoriano pasa en promedio 18,50 minutos por día en Facebook y revisa 8,83 páginas por visita. Es la red social que más tiempo capta de los ecuatorianos, seguida de Youtube (We are Social y Hootsuite, 2020).

Gráfico 2 Uso de las redes sociales

Fuente: Recuperado de: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-ecuador-en-el-2020-2021/

2.11 REGULACIÓN DE LAS REDES SOCIALES

La creación y utilización de las redes sociales que permiten la comunicación e interrelación con los demás se ha convertido en un gran fenómeno del siglo XXI, de allí la importancia de la regulación de las redes, pero también de las plataformas digitales a nivel mundial aun cuando en varios ya existe normativa que permita reducir el impacto de las actividades de las redes que atentan contra los derechos humanos.

Las redes sociales virtuales debido a la magnitud que han alcanzado están llevando a los gobiernos a preguntarse sobre el verdadero alcance y suficiencia de la regulación a internet y a las redes debido a los grandes riesgos y amenazas que tienen los usuarios.

Las leyes aplicables a las redes sociales tanto nacionales como internacionales al momento resultan ineficaces e insuficientes debido a la cantidad de acciones que se realizan en estas plataformas digitales. Las normativas que se propone para regular estas redes se debaten entre la regulación y la autorregulación y crean una evidente inseguridad jurídica (Arévalo, 2011, pag. 2-28).

CAPITULO III: DELITO INFORMÁTICO, CIBERACOSO Y LEGISLACIÓN ECUATORIANA

La modernización en los últimos años ha conducido a un manejo más acelerado de la comunicación entre las personas a través de la utilización de dispositivos tecnológicos como: ordenadores, tabletas, móviles, etc., pero al mismo tiempo ha puesto estos medios en manos de sujetos para perpetrar y facilitar diversas actividades delictivas que ponen en peligro o atentan contra la vida, la dignidad, la propiedad de las personas, entre otros derechos fundamentales.

Estas herramientas tecnológicas al ser utilizadas por personas que no tienen un claro comportamiento de coexistencia social puedan tener consecuencias devastadoras para las víctimas.

3.1. CONCEPTO DE DELITO INFORMÁTICO

Existen muchas definiciones de delito informático como por ejemplo la de Camacho Losa citada por Leyre Hernández (2009, pág. 231) en la que se manifiesta:

> 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.

Por su parte Marcelo Huerta Miranda y Claudio Líbano Mansur, en su obra "Los delitos Informáticos" (2004, pág. 13), definen al delito informático como:

> Todas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la victima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos.

Como podemos apreciar de las dos definiciones, el delito informático es un hecho criminal que se comete a través del uso de internet y de las redes sociales con la ayuda de una computadora, un teléfono inteligente o cualquier medio tecnológico o informático para intimidar a otros.

3.2 TIPOS DE DELITOS INFORMÁTICOS

Los delitos informáticos son de varias modalidades tal como se indican en la página web de la INTERPOL que a continuación se detallan: (a) Ataques contra sistemas y datos informáticos. (b) Usurpación de la identidad. (c) Distribución de imágenes de agresiones sexuales contra menores. (d) Estafas a través de Internet. (e) Intrusión en servicios financieros en línea. (f) Difusión de virus Botnets (redes de equipos infectados controlados por usuarios remotos) Phishing (adquisición fraudulenta de información personal confidencial),

Con respecto al uso de las redes sociales y el acceso a la información igualmente la INTERPOL cita que se consideran como delitos informáticos: (i) Acceso a material inadecuado (ilícito, violento, pornográfico, etc.). (ii) Robos de identidad. (iii) Acoso (pérdida de intimidad). (iv) Ciberbullying (acoso entre menores por diversos medios: móvil, Internet, videojuegos, etc.). (v) Cibergrooming (método utilizado por pederastas para contactar con niños y adolescentes en redes sociales o salas de chat)

3.3 DELINCUENTES CIBERNÉTICOS Y SUS OBJETIVOS

La ciberdelincuencia crece aceleradamente y trae consigo nuevas tendencias lo que convierte a los ciberdelincuentes en personas muy rápidas pues saben cómo explotar las nuevas tecnologías, utilizar nuevos métodos de ataque y coordinar ataques en minutos lo que les lleva a convertirse en sujetos muy peligrosos.

Jesús Alberto Loredo González (2003, pág. 46) en su estudio relacionado con los delitos informáticos, manifiesta que “así como existen una gran cantidad de delitos relacionados con el uso de sistemas informáticos, también existe una

amplia gama de delincuentes.” Considerando lo manifestado, Loredo define dos clasificaciones de delincuentes: la primera aquellos que son expertos en seguridad informática o llamados hackers y en el segundo grupo se encuentran aquellos que utilizando el anonimato llevan a cabo acciones poco éticas como es el acoso, el cyberbullying, pornografía infantil, turismo sexual ente otras.

3.4 EL CIBERACOSO COMO DELITO

El acoso cibernético, ciberacoso, ciberbulling como se lo quiera denominar no es más que un tipo de violencia que hace uso de la información electrónica que mantiene un usuario de internet, de correo electrónico, redes sociales, blogs, mensajería instantánea, mensajes de texto, teléfonos celulares o móviles, tabletas, para hostigar, perseguir, asediar a un sujeto o grupo de sujetos de manera constante, a través de ataques personales, burlas, amenaza, persecución, calumnias, difamación, falsedades, mentiras, etc., a la víctima.

El ciberacoso es considerado de gravedad toda vez que tiene una cantidad ilimitada de receptores, menores de edad en su gran mayoría aunque también se observa en adultos, este tipo de violencia como vemos no tiene tiempo, no mide fronteras, pues, una vez difundidos los contenidos, se vuelven virales rápidamente y son casi imposibles de borrarlos.

La violencia cibernética o ciberacoso en el transcurso de los últimos años se ha desarrollado ampliamente al punto de observarse diversos tipos como el *grooming*, sextorsión, difusión de mensajes de sexting, ciberviolencia de género, ciberbullying entre los más reconocidos, tipos de ciberacoso que en muchos países se encuentran regulados en un marco legal como es el caso de España en el cual los acosadores son objeto de sanciones como se establece en el artículo 131 de la Ley 26.904 del Código Penal y en el caso de menores de edad se aplica el artículo 183 ter de la Ley Orgánica 10/1995 de 23 de noviembre, del Código Penal (Departamento de Periodismo y Comunicación Audiovisual de la Universidad Rey Juan Carlos. 2022)

En nuestro país lamentablemente el ciberacoso es un tipo de conducta delictiva que no se encuentra tipificada como delito informático ya que no hay figura legal que lo tipifique.

Para que el ciberacoso sea considerado un delito en la legislación ecuatoriana, el tratadista Eugenio Cuello Calón, en su obra titulada “Derecho Penal”, al hablar sobre la tipicidad manifiesta que:

> Debido a que producido el hecho se deberá investigar si el mismo está previsto y penado como delito o como falta en la ley penal es decir indagar si se trata de un hecho típico o como dice el código si está sancionado por la ley penal pues la ley es la única fuente del Derecho Penal Ecuatoriano, quedando excluido la analogía y la interpretación extensiva (Cuello, 1953).

Como se puede apreciar, el jurista manifiesta que el hecho que se perpetre ya sea acción u omisión debe estar tipificado en la ley penal para que sea considerado como delito en virtud con el principio de legalidad que rige al derecho penal.

Por su parte Francisco Muñoz Conde, en su obra “Teoría General del Delito“, se refiere a la tipicidad y explica que “solo los hechos tipificados en la ley penal como delitos pueden ser considerados como tal” (Conde F. M., 2016, pág. 16).

El Art. 76 Núm. 3 de la Constitución de la República del Ecuador, que trata sobre el principio de legalidad, de la siguiente forma:

> Nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley. Sólo se podrá juzgar a una persona ante un juez o autoridad competente y con observancia del trámite propio de cada procedimiento (Constitución de la República del Ecuador, 2008).

Como podemos apreciar el artículo en mención expresa que ninguna persona será juzgada por un acto que no esté tipificado en la ley.

3.5 TIPOS DE CIBERACOSO

De acuerdo con Nancy Willard (2007) citado por Guillermo Cárdenas en su artículo denominado “Ciberacoso” , esta conducta va desde el flaming al cyberstalking siendo los más conocidos el sexting, ciberbullying y el Grooming como se describe a continuación:

a.- Flaming: Enviar mensajes electrónicos con lenguaje vulgar, o discursos incendiarios para incitar a la pelea.

b.- Acoso: Que incluye además mensajes ofensivos, que se prolongan por más tiempo.

c.- Denigración: Generar y difundir mentiras sobre alguien para destruir su reputación o alejar a sus amistades.

d.- Imitación o enmascaramiento: Donde el agresor finge ser otra persona para destruir la reputación o relaciones sociales de la víctima.

e.- Cyberstalking (persecución cibernética): Incluye altos niveles de intimidación o amenazas de daño que hacen a la víctima temer por su seguridad.

f.- Outing: En el cual se comparten sin permiso secretos o información comprometedora sobre la víctima, incluyendo fotos y mensajes

g.- Engaño: El acosador usa mentiras para que la víctima revele información personal muy delicada. La estafa y el abuso de confianza guarda relación con el engaño toda vez que se entrega una cosa de propiedad de ella o de propiedad de una tercera persona, de forma libre y voluntaria con lo cual se le despoja a la personas de sus bienes

h.- Exclusión: Son actos intencionados para mantener a la víctima excluida o alejada del grupo.

i.- El Grooming: Son estrategias que utiliza una persona adulta para ganarse la confianza de otra persona especialmente más joven y adquirir el control y poder sobre el o ella de manera especial para extorsionarla sexualmente a través del engaño como por ejemplo conseguir que se desnude frente a la webcam o que le envíe fotos desnudo o desnuda; una vez obtenido lo deseado inicia el chantaje es decir comienza a manipular a su víctima con amenazas de que va a publicar el material fotográfico sexual que le fue enviado. (Bennett, 2014.)

j.- El Ciberbullying: ciberviolencia o violencia virtual es la forma a través de la cual los medios de comunicación virtual: internet, telefonía móvil, sitios web, videojuegos en línea, redes sociales, favorecen el ejercicio de la violencia sobre otras personas a través uso del anonimato o el ocultamiento, por lo general este tipo de violencia es la continuación del maltrato presencial que ya fuera ejecutado. Este modo de violencia implica un grave e impactante daño sobre la víctima. Esta forma de violencia se manifiesta cuando el engañador o acosador pública a través de internet o de las redes una imagen, video, datos privados y cualquier información que pueda perjudicar o avergonzar a la víctima o también hacerse pasar por otra persona creando un perfil falso que le sirva para dar a conocer datos privados de la víctima o causar daño a terceras personas (Abufhele, 2008, pág.31-42).

k.- Publicaciones sin consentimiento de contenido el Sexting: Es una estrategia utilizada a través de la cual se comparte imágenes de tipo sexual personal o de terceros mediante el uso de teléfonos móviles o internet, el mayor riesgo es que dicho material sea publicado y se viralice sin autorización, quedando la intimidad de la víctima expuesta ante millones de usuarios. Las consecuencias de este acto son graves a corto y largo plazo para la víctima (CCMA, 2010).

3.6.- ANÁLISIS DE LA LEGISLACIÓN ECUATORIANA

La tecnología es un proceso que tiene por objeto transformar o cambiar lo existente con el fin de crear algo nuevo u otorgarle otra función (Calispa 2019). Hay que subrayar que la tecnología al estar más junto a los sujetos estos se han visto acorralados toda vez que su uso agilita procesos, acorta tiempos, educa, informa, pero al mismo tiempo que aproxima y aparta a los individuo y es capaz de complicar y atentar contra su vida debido al mal uso que está siendo dado por delincuentes cibernéticos.

De acuerdo con Diego Fernando Posso López en su estudio sobre Los Delitos Informáticos y la Violación de los Derechos Constitucionales del Ofendido, manifiesta la existencia de nuevas formas delictivas que antes no existían como consecuencia del avance de la informática y de los medios electrónicos la

normativa vigente resulta muy limitada para prevenir y sancionar estas nuevas formas delictivas.

Como ya se dijo en el anterior capítulo, en el Ecuador no existe una ley ni se ha tipificado adecuadamente los delitos informáticos, así como tampoco establece sanciones al ciber delincuente y protección al cibernauta, por lo tanto existen vacíos legales dentro del COIP y de otras leyes más aún si se trata sobre el ciberacoso, conducta que no ha sido regulada a pesar de ser lesiva, descriptible y demostrable.

Por lo expuesto a continuación se analizan de forma breve la leyes ecuatorianas, partiendo desde la Constitución de la República 2008

a.- Constitución de la República del Ecuador

Para un país, es importante mantener a convivencia social y el respeto y cumplimiento a las normas y leyes lo que se convierten en la base fundamental para un Estado Constitucional de Derecho que se torna efectivo con respecto al cumplimiento de sus principios básicos, lo que está en relación a la violación de las leyes o normas por parte de las personas sobre los cuales rigen los principios del Derecho y donde el –Estado ejerce el ius puniendi cuando se ha transgredido la reglas que rigen las conducta delos individuo. El artículo 75 de la Constitución de la República al respecto de lo manifestado señala:

> Toda persona tiene derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en indefensión. El incumplimiento de las resoluciones judiciales será sancionado por la Ley. (Constitución de la República del Ecuador, 2008)

La Constitución de la República como mandato establece que todos los principios y derechos son inalienables, irrenunciables, indivisibles, interdependientes y de igual jerarquía, y además son de aplicación directa y de obligatorio cumplimiento por parte de todo individuo.

El Artículo 16 numerales 2 y 4 de la Constitución en lo relativo a la comunicación e información expresa que todas las personas tienen derecho a:

> "(…) 2. El acceso universal a las tecnologías de la información y comunicación.
> 4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad." (Constitución de la República del Ecuador, 2008)

En el artículo 19 se plantea que:

> La ley regulará la prevalencia de contenidos con fines informativos, educativos y culturales en la programación de los medios de comunicación, y fomentará la creación de espacios para la difusión de la producción nacional independiente. Se prohíbe la emisión de publicidad que induzca a la violencia, la discriminación, el racismo, la toxicomanía, el sexismo, la intolerancia religiosa o política y toda aquella que atente contra los derechos (Constitución de la República del Ecuador, 2008).

Por su parte en el numeral 3, se manifiesta que:

> Los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte.
> Para el ejercicio de los derechos y las garantías constitucionales no se exigirán condiciones o requisitos que no estén establecidos en la Constitución o la ley.
> Los derechos serán plenamente justiciables. No podrá alegarse falta de norma jurídica para justificar su violación o desconocimiento, para desechar la acción por esos hechos ni para negar su reconocimiento. (Constitución de la República del Ecuador, 2008)

Y el numeral 8 menciona que:

> El contenido de los derechos se desarrollará de manera progresiva a través de las normas, la jurisprudencia y las políticas públicas. El Estado generará y garantizará las condiciones necesarias para su pleno reconocimiento y ejercicio (Constitución de la República del Ecuador, 2008).

Continuando con el análisis, el artículo 66 de la Constitución en relación con los derechos de libertad en el numeral 3 literales a y b garantiza:

> El derecho a la integridad personal, que incluye:
>
> a) La integridad física, psíquica, moral y sexual.
>
> b) Una vida libre de violencia en el ámbito público y privado. El Estado adoptará las medidas necesarias para prevenir, eliminar y sancionar toda forma de violencia, en especial la ejercida contra las mujeres, niñas, niños y adolescentes, personas adultas mayores, personas con discapacidad y contra toda persona en situación de desventaja o vulnerabilidad; idénticas medidas se tomarán contra la violencia, la esclavitud y la explotación sexual. (Constitución de la República del Ecuador, 2008)
>
> El numeral 18, del Artículo 66 garantiza:
>
> El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona. (Constitución de la República del Ecuador, 2008) mientras que el numeral 19 establece El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Constitución de la República del Ecuador, 2008)

b.- Tratados y Convenios de Derechos Humanos

b.1 Convención Interamericana sobre Derechos Humanos

El artículo 11.- Protección de la Honra y de la Dignidad: en los numerales 1, 2, 3 que también están está en el artículo 12 de la Declaración Universal de los Derechos Humanos ONU, 10-12-1948 (Naciones Unidas, s.f.) establecen:

> 1. “Toda persona tiene derecho al respecto de su honra y al reconocimiento de su dignidad.”
>
> 2. “Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación”.
>
> 3. “Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques” (José. s.f.).
>
> Artículo 13. Libertad de Pensamiento y de Expresión
>
> 1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
>
> 2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:
>
> a) el respeto a los derechos o a la reputación de los demás, o
>
> b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.
>
> 3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones esos ataques”.

En la Declaración Universal de los Derechos Humanos se puede observar que varios de los derechos considerados prioritarios como son: el derecho a la

libertad de expresión, el derecho a la privacidad y a estar libre de difamación y el derecho a vivir libre de violencia, actualmente son vulnerados en el ciberacoso así por ejemplo podemos ver como a través de las redes sociales se limita el derecho a la expresión y libre opinión de un individuo cuando este no está de acuerdo con lo manifestado. El ciberacosador cuya tarea es destruir a su víctima vulnera su derecho a la expresión al punto de generar el rechazo de los cibernautas.

Otro derecho vulnerado es el contemplado en el artículo 12 de la Declaración de los Derechos Humanos y es el derecho a la privacidad y a estar libre de difamación, en este caso el acosador se aprovecha del anonimato que le brinda el internet y las redes para ingresar a la información personal de su víctima con lo cual no solo violenta su privacidad sino también su buen nombre que suele ser utilizado en su contra.

b.2 Pacto Internacional de Derechos Civiles y Políticos (ONU)

El Pacto Internacional de Derechos Civiles y Políticos entró en vigencia en el año 1976 es muy claro en la protección de los derechos humanos y de las libertades fundamentales de las personas como se establece a continuación:

> Artículo 17
>
> 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
> 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

El artículo hace referencia a que todas las personas deben recibir protección de la ley ante ataques de cualquier índole e incluso nadie puede tener intromisiones en su vida, su domicilio, correspondencia que incluye la digital, su honra y su reputación

Artículo 19

1. Nadie podrá ser molestado a causa de sus opiniones.
2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a) Asegurar el respeto a los derechos o a la reputación de los demás;" (Pacto Internacional de Derechos Civiles y Políticos).

El Pacto Internacional de Derechos Civiles y Políticos, enfatiza sobre el derecho de la libertad de expresión sin recibir ningún tipo de críticas, insultos, comentarios ofensivos, controlar esto en las redes sociales es muy complicado, toda vez que hay personas que utilizan perfiles falsos y se escudan en el anonimato para difamar, humillar, ofender a otras personas que piensan diferente, así pues la ley restringe de alguna manera este tipo de conductas.

b.3 Convenio sobre la Ciberdelincuencia Convenio de Budapest

Este convenio tiene por objeto garantizar la acción penal y los derechos humanos enunciados y consagrados en todos los convenios sobre derechos humanos con la finalidad de defender la opinión, la libre expresión, respeto a la vida privada, la protección de datos personales.

Nuestro país lamentablemente no se encuentra formando parte de este Convenio que entro en vigor en el 2004 mismo que instaura una política penal común y de cooperación internacional para frenar los delitos informáticos. Chile, nivel de Sudamérica el país que ha tenido buenos resultados con la firma del convenio pues ha sido la plataforma para discutir y modernizar la legislación ante la escasa regulación

Existente (BID. 2020, págs.45-174).

c. Código Orgánico Integral Penal

El Código Orgánico Integral Penal COIP, es el cuerpo normativo supremo en materia de Derecho Penal que rige al Ecuador desde su vigencia en el 2014. Es una norma de naturaleza sustantiva y adjetiva en materia penal, del delito, de la pena, tipificando y sancionando las conductas delictivas existentes en el país. Debido a que el Internet es un escenario que ha permitido se expanda la delincuencia informática, para los Estados el enfrentar estos delitos es un reto por cuanto la tecnología sigue evolucionando lo que no permite su sanción de forma pertinente.

El COIP vigente tipifica varios delitos vinculados con el uso de la tecnología así tenemos:

En el artículo 234 que "el acceso no consentido a un sistema informático, telemático o de telecomunicaciones" en contra de la voluntad de su legítimo titular con el fin de explotar, modificar, desviar datos o acceder a servicios evitando el pago a sus proveedores será sancionado con tres a cinco años de privación de libertad (COIP 2014).

La amenaza y la calumnia figuras jurídicas sujetas a sanción penal, cuando se dan a través de las redes sociales es muy complicada su penalización toda vez que en la norma jurídica penal no está tipificado en este contexto. En cuanto al *child grooming* o *acoso sexual* a menores utilizando el internet tampoco se encuentra tipificado o regularizado en la norma jurídica (Puyol, 2019. Pag.).

En relación con lo anteriormente expresado, el artículo 173 establece:

> Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos. - La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años.
>
> Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años.

> La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años. (COIP 2014).

El artículo que antecede se relaciona con el ciberacoso por el hecho de que el ciberacosador pueden crearse perfiles en redes sociales falsos, suplantando la identidad de otras personas con el objeto de acosar, establecer comunicaciones de contenido sexual, ya sea de forma coactiva o intimidatoria; la mayoría de los acosadores instigan a las personas menores de edad que son más vulnerables ante estas situaciones.

El utilizar fuerza, intimidación, coacción y hasta la violencia son medios para el cometimiento de estos delitos ya que lamentablemente el menor confía de la identidad de la persona que está frente a ella a través de medios informáticos.

En cuanto a la falsa identidad, el uso de las redes sociales facilita el fraude, el engaño, la estafa. Esta última que se sanciona con tres a cinco años de privación de libertad conforme se cita en el artículo 186, pero bajo el uso del anonimato y sin pruebas suficientes esta figura insuficiente para ser considerado delito cibernético.

El articulo 190 Apropiación fraudulenta por medios electrónicos manifiesta que:

> La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.
>
> La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas,

> utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes (COIP 2014)

Por su parte el artículo 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos manifiesta que:

> La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años. (COIP 2014)

Artículo 178.- Violación a la intimidad

> La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley. (COIP 2014)

Reiteradamente a través de internet y de las redes sociales en especial se evidencia la violación a la intimidad personal cuando se reenvía y difunden mensajes de voz, audio, video y fotos los cuales se viralizan en segundos causando daño a sus víctimas psicológicos, incluso hasta llevarlos a suicidarse.

d. Código de la Niñez y Adolescencia.

El Código de la Niñez y Adolescencia entrado en vigencia en junio del 2003 tiene como finalidad de conformidad con el artículo 1 brindar a los niños, niñas y adolescentes protección de parte del Estado y garantizar que sus derechos y obligaciones sean cumplidas y tengan un desarrollo integral.

Lastimosamente, en la Constitución del Ecuador, el Código de la Niñez y Adolescencia y la Ley de Educación Intercultural no existe normativa específica sobre el ciberacoso en este grupo vulnerable, lo que más se acerca a este es el término “acoso”.

A continuación, se analizan los siguientes artículos.

En el Art. 6.- Igualdad y no discriminación, manifiesta lo siguiente:

> Todos los niños, niñas y adolescentes son iguales ante la ley y no serán discriminados por causa de su nacimiento, nacionalidad, edad, sexo, etnia; color, origen social, idioma, religión, filiación, opinión política, situación económica, orientación sexual, estado de salud, discapacidad o diversidad cultural o cualquier otra condición propia o de sus progenitores, representantes o familiares. El estado adoptara las medidas necesarias para eliminar toda forma de discriminación. (Código de la Niñez y Adolescencia, 2003)

Como es conocido un factor importante para que se de el ciberacoso entre los niños niñas y adolescentes de la discriminación por parte de sus pares de allí que el artículo que antecede el Estado será el encargado de tomar las medidas necesarias para erradicarla

En el Art. 8.- Corresponsabilidad del Estado, la sociedad y la familia,

> Es deber del Estado, la sociedad y la familia, dentro de sus respectivos ámbitos, adoptar las medidas políticas, administrativas, económicas, legislativas, sociales y jurídicas que sean necesarias para la plena vigencia, ejercicio efectivo, garantía, protección y exigibilidad de la totalidad de los derechos de niños; niñas y adolescentes.
>
> El Estado y la sociedad formularán y aplicarán políticas públicas sociales y económicas; y destinarán recursos económicos suficientes, en forma estable, permanente y oportuna. (Código de la Niñez y Adolescencia, 2003)

De acuerdo con lo citado en este artículo se faculta al Estado, la sociedad y la familia para que tome las medidas necesarias que permitan las vigencias de los

derechos de los niños niñas y adolescentes, con el objeto de que los menores de edad tengan una buena formación durante su desarrollo

Art. 50.- Derecho a la integridad personal.

> Los niños, niñas y adolescentes tienen derecho a que se respete su inte gridad
> personal, física, psicológica, cultural, afectiva y sexual. No podrán ser sometidos a torturas, tratos crueles y degradantes (Código de la Niñez y Adolescencia, 2003).

Este artículo es muy claro cuando manifiesta que los niños, niñas y adolescentes tiene derecho a que se respete su integridad física, psicológica, cultura, afectiva y emocional, en el caso del ciberacoso, este derecho es vulnerado cuando se utilizan medios telemáticos y más aún cuando la tecnología ha avanzado rápidamente y los menores hacen uso de celulares, Tablet, computadores entre otros.

Art. 67.-Concepto de maltrato.

> Se entiende por maltrato toda conducta, de acción u omisión, que provoque o pueda provocar daño a la integridad o salud física, psicológica o sexual de un niño, niña o adolescente, por parte de cualquier persona, incluidos sus progenitores, otros parientes, educadores y personas a cargo de su cuidado; cualesquiera sean el medio utilizado para el efecto, sus consecuencias y el tiempo necesario para la recuperación de la víctima. Se incluyen en esta calificación el trato negligente o descuido grave o reiterado en el cumplimiento de las obligaciones para con los niños, niñas y adolescentes, relativas a la prestación de alimentos, alimentación, atención médica, educación o cuidados diarios; y su utilización en la mendicidad. (Código de la Niñez y Adolescencia, 2003)
>
> Maltrato psicológico es el que ocasiona perturbación emocional, alteración psicológica o disminución de la autoestima en el niño, niña o adolescente agredido. Se incluyen en esta modalidad las amenazas de causar un daño en su persona o bienes o en el de sus progenitores, otros parientes o

> personas encargadas de su cuidado (Código de la Niñez y Adolescencia, 2003)

El internet y por ende las redes sociales se ha convertido en un medio que permite provocar daños a la integridad física, psicológica y sexual de los niños niñas y a adolescentes a través del ciberacoso o violencia cibernética, pero esto no se encuentra normado jurídicamente en nuestro país por lo que ha llevado a que los menores tengan graves problemas sobre todo psicológicos que puedan llevarlos incluso a querer suicidarse.

En el Art. 305.- Inimputabilidad de los adolescentes

> Los adolescentes son penalmente inimputables y, por tanto, no serán juzgados por jueces penales ordinarios ni se les aplicarán las sanciones previstas en las leyes penales (Código de la Niñez y Adolescencia, 2003).

El artículo señala que los adolescentes son inimputables penalmente, pues no han cumplido la mayoría de edad, toda vez que esta es un factor esencial en el campo jurídico que permita determinar si una persona tiene capacidad y responsabilidad penal.

En el Art. 306.- Responsabilidad del adolescente.

> Los adolescentes que cometan infracciones tipificadas en la ley penal estarán sujetos a medidas socioeducativas por su responsabilidad de acuerdo con los preceptos del presente Código (Código de la Niñez y Adolescencia, 2003).

Los adolescentes al ser penalmente inimputables, no están exentos de una sanción por su mala conducta, el Código de la Niñez y Adolescencia establece sanciones socioeducativas.

En el Art. 307.- Inimputabilidad y exención de responsabilidad de niños y niñas, manifiesta lo siguiente:

> Los niños y niñas son absolutamente inimputables y tampoco son responsables; por tanto, no están sujetos ni al juzgamiento ni a las medidas socio - educativas contempladas en este Código. (Código de la Niñez y Adolescencia, 2003)

Al ser la edad de gran importancia al momento de determinar la responsabilidad que tengan los niños y las niñas de ninguna forma serán sancionados por las medidas socioeducativas establecidas el Código de la Niñez y Adolescencia.

e. Ley Orgánica de Educación Intercultural (LOEI)

Art. 2.- Principios

d. Interés superior de los niños, niñas y adolescentes.

El interés superior de los niños, niñas y adolescentes, está orientado a garantizar el ejercicio efectivo del conjunto de sus derechos e impone a todas las instituciones y autoridades, públicas y privadas, el deber de ajustar sus decisiones y acciones para su atención. Nadie podrá invocarlo contra norma expresa y sin escuchar previamente la opinión del niño, niña o adolescente involucrado, que esté en condiciones de expresarla.

t. Cultura de paz y solución de conflictos. - El ejercicio del derecho a la educación debe orientarse a construir una sociedad justa, una cultura de paz y no violencia, para la prevención, tratamiento y resolución pacífica de conflictos, en todos los espacios de la vida personal, escolar, familiar y social. Se exceptúan todas aquellas acciones y omisiones sujetas a la normatividad penal y a las materias no transigibles de conformidad con la Constitución de la República y la Ley.

Art. 8.-Obligaciones. - Las y los estudiantes tienen las siguientes obligaciones

e. Tratar con dignidad, respeto y sin discriminación alguna a los miembros de la comunidad educativa;

l. Denunciar ante las autoridades e instituciones competentes todo acto de violación de sus derechos y actos de corrupción, cometidos por y en contra de un miembro de la comunidad educativa. La presente ley determina los principios y fines generales que orientan a la educación al marco toda una vida, tomando en cuenta de intercultural, plurinacional y evaluación; enfatizando así los derechos, obligaciones y garantías constitucionales en el ámbito educativo.

Como podemos ver en esta ley si bien toma muy encuentra lo derechos deberes y garantías que tienen los niños niñas y adolescente en el contexto educativo, no hace referencia al ciberacoso que actualmente se está registrando en este grupo vulnerable.

Iv conclusiones

En el Ecuador así como en el resto del mundo, el uso del internet y por ende de las redes sociales han venido a ser parte de la vida social virtual y personal de los seres humanos lo cual ha sido aprovechada para comunicar e informara en amplios campos como el social, económico, legal, pero también se ha aprovechado para llevar a cabo actos delictivos y discriminatorios como es el caso del ciberacoso o violencia cibernética, los fraudes, el engaño, el uso de información personal, entre otros por lo que se torna necesario regular el uso de este medio de comunicación.

Actualmente en el país existe una amplia diversidad de delitos informáticos en ejecución lo cual ha dejado en la indefensión a miles de usuarios del internet y de la redes sociales al vulnerarse de manera repetitiva su derecho a la intimidad que de alguna manera ha sido protegida en el ámbito jurídico, sin embargo, se requiere reforzar las seguridades desde el campo informático y desde el ámbito legal, formulándose una normativa que brinde seguridad a los cibernautas.

Las reformas realizadas al Código Orgánico Integral Penal han traído una serie de cambios en lo que tienen que ver con los procedimientos y tipificación de los delitos informáticos, sin embargo es necesario se tome en cuenta el avance de la tecnología debido uso intensivo del internet y la redes sociales que han llevado a que se vulnere la información personal y ser utilizada sin autorización.

Como se ha podido apreciar de la investigación realizada, en el país no se encuentra tipificado como delito el ciberacoso o violencia cibernética por lo que se debería incluir en el COIP normas que sancionen a los individuos que cometen este tipo de delito ya que vulneran bienes jurídicos como lo manifiesta la legislación ecuatoriano.

La investigación que se centra en la violencia cibernética y su problema de no tipificación dentro de la normativa legal, no es por falta de estos actos ya que existen un sinnúmero de casos muchos de los cuales no han sido reportados, sin embargo, la justicia ha tomado medidas para precautelar la intimidad de las personas a través de subnormas dentro de sus leyes.

La conducta humana debe estar tipificada en el ordenamiento jurídico penal para ser relevante en su ámbito, de allí que dicha conducta debe ser incluida en un tipo penal para posteriormente ser considerada antijurídica. Por ello, regular una conducta típica es necesario en la Legislación Penal, ya que sin ella no se puede estipular lo prohibido y establecer una norma que sancione.

La tipicidad es el elemento principal para configurar un delito pues sin este elemento que hace que la conducta sea visible y resulta en el accionar, cuando carece del tipo es improbable su punibilidad basándose en el principio de legalidad ya que por definición para que un acto sea considerado delitos debe estar tipificado en la ley, sino es considerado atípico. Este elemento se divide en dos: la tipicidad objetiva y la tipicidad subjetiva.

La tipicidad objetiva comprende, la descripción de la persona que realiza el tipo (sujetos), la conducta típica y el resultado (objeto material) en el caso de los delitos de resultado, en otras palabras es la que establece si la conducta realizada por el sujeto fue cometida por culpa o dolo. Aquí encontramos al (i) Sujeto activo del delito que es la persona que realiza el tipo, pudiendo ser hombre o mujer que en el caso del ciberacoso utiliza los medios tecnológicos para acosar a su víctima; se entendería entonces que es un delito cometido a través de un recurso. Tecnológico. (ii) el sujeto pasivo del delito será la cualquier persona que fue objeto del ciberacoso a través de un recurso tecnológico.

En la tipicidad Subjetiva, se examina el aspecto interno del individuo que cometido el tipo penal, se analiza el dolo, la culpa, los elementos subjetivos del tipo. El tipo penal puede ser doloso o culposo, dependiendo si el sujeto tiene conciencia y voluntad de realizar lo que está detallado en el tipo penal objetivo, o si el actor no observó el deber objetivo de cuidado.

V. Recomendaciones

Conforme a lo investigados vemos que existen diversas formas de delitos informáticos que se cometen a través de medios tecnológicos por lo que es preciso que en la legislación ecuatoriana, se reforme la normativa de tal manera que se pueda sancionar estos delitos toda vez que debido a los vacíos jurídicos existentes en la normativa estos quedan en la impunidad.

Es importante también que a nivel de la Asamblea Nacional, se considere la creación de una ley específica que sanciones estos delitos y se implementen mecanismos de protección para las víctimas mediante la revisión de la actual Ley de Comercio Electrónico, Mensajes de Datos y Firma Digital.

Es indispensable que la Asamblea Nacional tipifique dentro del Código Orgánico Integral Penal, el ciberacoso, lo que permitirá una regulación completa sobre este tipo de delito que ha colocado a nuestro país dentro de modalidades criminales tecnológicas no tipificadas como el resto de países del mundo.

El Gobierno debería implemente políticas de Estado con el objeto de concientizar a la ciudadanía sobre la problemática de la violencia por el uso de las TIC y se promuevan proyectos de ley que regulen y sancionen estas prácticas de acoso, o cualquier tipo de intimidación debido al uso de la tecnología y sus medios.

Referencias bibliográficas

Abufhele, M; Arab, E. (2008). *El fenómeno del "Bullying". Caracterización del problema y sus estrategias de intervención".* Revista Chilena de Psiquiatría y Neurología de la Infancia y Adolescencia, volumen 19-no1. (Pág. 31-42) https://cienciadigital.org/revistacienciadigital2/index.php/exploradordigital/article/view/ 332 (Recuperado. El 10 de enero de 2022).

Alvino C. (2021). Est*adísticas de la situación digital de Ecuador en el 2020-2021.* Branch Group. Agencia de Marketing Digital Medellín Colombia. https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-ecuador-en-el-2020-2021/. Artículo (Recuperado. El 15 de enero de 2022).

Alberdi. I. y Matas. N. (2002), *Informe sobre malos tratos a mujeres en España*, Colección de Estudios Sociales N°10, Fundación "La Caixa", de: españa.www.estudios.lacaixa.es https://repositorio.flacsoandes.edu.ec/bitstream/10469/ 11859/9/ TFLACSO-016LFR.pdf (Recuperado. El 5 de enero de 2022).

Arévalo. M. (2011*). Modelos de regulación jurídica de las redes sociales virtuales*. VIA IURIS. https://www.redalyc.org/pdf/2739/273922799007.pdf (Recuperado. El 13 de marzo 2022).

Avilés, J. (2005). Estudio de la incidencia de la intimidación y el maltrato entre iguales en la educación secundaria obligatoria mediante el cuestionario Canales de Psicología, Pág. (21-27-41). . (Recuperado. El 12 de marzo 2022).

Bennett N. (2014) *Conceptual and Measurement Issues. J Child Sex Abus.* O'Donohue W. The Construct of Grooming in Child Sexual Abuse. PubMed PMID. Págs. (-) https://www.sciencedirect.com/science/article/pii/S0716864015000048#bib0110 (Recuperado. El 8 de diciembre 2021).

BID. (2020). *CIBERSEGURIDAD. RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE*. Págs. (45-174). https://publications.iadb.org/publications/spanish/document/Reporte-

Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

Burgess, A. W. y Baker T. (2008). *Stalking and Psychosexual Obsession: Psychological Perspectives for Prevention, Policing and Treatment.* Nueva York: Wiley. Págs. (554-555) https://onlinelibrary.wiley.com/doi/book/10.1002/9780470713037 (Recuperado. El 11 de diciembre 2021).

Cárdenas, G. (2006). *CIBERACOSO*. Revista digital comoves. http://www.comoves.unam.mx/assets/revista/197/ciberacoso.pdf (Recuperado. El 10 de enero 2022).

Carrasco, R., & Navas, O. (2013). *El Acoso Escolar A Través De Las Nuevas Tecnologías. El Cyberbullying.* Pág 3-4. Yumpu. https://www.yumpu.com/es/docu ment/read/14450088/el-acoso-escolar-a-traves-de-las-nuevas-ticemur. (Recuperado. El 10 de marzo 2022).

Castells, P. (2007). *Víctimas y Matones, claves para afrontar la violencia en niños y jóvenes*. Ediciones CEAC. Págs. (27-34-73-78-80-82-84-97-179). http://www.redage.org/publicaciones/victimas-y-matones-claves-para-afrontar-la-violencia-en-ninos-y-jovenes (Recuperado. El 12 de marzo 2022).

Ciberintocables. (2022) *El Ciberacoso en el Código Penal.* Periodismo y Comunicación Audiovisual de la Universidad Rey Juan Carlos https://ciberintocables.com/ciberacoso-codigo-penal/ (Recuperado. El 5 de enero 2022).

Consejo de la Judicatura. (2016). *Conoce tus derechos.* Función Judicial. https://www.funcionjudicial.gob.ec/pdf/conoce-tus-derechos.pdf (Recuperado. El 4 de diciembre 2021).

Dupret, M. (2012). *Violencia familiar contra los niños: respuestas institucionales.* Universitas Revista de Ciencias Sociales y Humanas. Pág. (20). https://revistas.ups.edu.ec/index.php/universitas/article/view/16.2012.01 (Recuperado. El 30 de noviembre 2021).

Escobar N. (2015). *Qué es el grooming y cómo podemos proteger a los niños en*

Internet. Hipertextual. https://hipertextual.com/2015/05/que-es-el-grooming (Recuperado. El 20 de diciembre de 2021).

FIB Facultat d'Informàtica de Barcelona. (2018). *Informática el pasado del futuro, historia del Internet*. FIB. https://www.fib.upc.edu/retro-nformatica/historia/int ernethtml (Recuperado. El 28 de noviembre 2021).

Garaigordobil, M. y Oñederra, J. A. 2010*. La violencia entre iguales. Revisión teórica y estrategias de intervención*. Pirámide. https://trasosdigital.files.wordpress.com /2013/07/articulo-violencia.pdf (Recuperado. El 23 de diciembre 2021).

García. M. (2011). *El acoso escolar diagnóstico y prevención.* Grupo editorial

siglo veintiuno. https://www.academia.edu/36896616/LIBRO_El_acoso_escolar . (Recuperado. El 10 de marzo 2022).

González, R. et. al. (2009*). Las redes sociales en ayuda de las Pequeñas y Medianas Empresas (PyMES)"*. Observatorio de la Economía Latinoamericana. Nº 120. (Recuperado. El 2 de diciembre 2021).

Gonzalez, L. (2010). *Responsabilidad Legal en Redes Sociales en Internet.* Legalit. Párr. (2-3). www.legalit.com.ar/responsabilidad-legal-en-redes-sociales-en-inter net-facebook-normas-leyeslegislacion-argentin. (Recuperado. El 22 de noviembre 2021).

Guzmán. A. (2011). *Ciberacoso: Causas y Consecuencias.* Articulo Congreso TIC. Párr. (6) http://congresoedutic.com/forum/topics/el-ciberacoso-causas-y (Recuperado. El 8 de diciembre de 2021).

Harris, S., & Petrie, G. (2006*). El acoso escolar. 3 ra Ed.* Ediciones Paidos Ibérica, S.A. Págs. (58-59). https://www.redalyc.org/pdf/802/80224034006.pdf (Recuperado. El 12 de marzo 2022).

Hennig M. Cuesta M. Fernández O. Dorival. M. *Cyberbullying, Detección Y Factores de análisis: Un estudio comparativo 2019.* Revista espacios. Pag.

(7). https://www.revistaespacios.com/a19v40n02/a19v40n02p04.pdf (Recuperado. El 10 de marzo 2022).

Loredo, J.A. (2013). *Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo.* Eprints. Pág. (46). http://eprints.uanl.mx/3536/1/Delitos_ informaticos.pdf (Recuperado. El 28 de noviembre 2021).

Madrid, et.al, 2020, Factores asociados al ciberacoso en adolescentes. Una perspectiva ecológico-social párr.(10). http://www.scielo.org.mx/scielo.php?script=sci_ arttext&pid=S018 5-269820200001 00068 (Recuperado. El 11 de marzo 2022).

Miranda, M. y Mansur, C. (2004). *Los Delitos Informáticos.* Jurídica Conosur. Pág. (13). http://biblioteca.usek.cl/cgi-bin/koha/opac-detail.pl?biblionumber=14490 (Recuperado. El 30 de diciembre 2021).

Mendoza, E. 2012. *Acoso cibernético o cyberbullying: Acoso con la tecnología electrónica.* Pediatría de México Vol. 14. Pág. (133) https://www.medigraphic.com/pdfs/conapeme/pm-2012/pm123g.pdf. (Recuperado. El 15 de diciembre 2021).

Muñoz Conde. F. (1984). *Teoria General del Delito*. Temis. Págs. (16). https://www.sijufor.org/uploads/1/2/0/5/120589378/06_mu%C3%91oz_conde_t _del_delito.pdf (Recuperado. El 15 de diciembre 2021).

Navarrete J. (2020*). Tipos de Redes sociales*. Imotione Lab. párr. 1. https://www.Inboundemotion.com/blog/author/jordi-navarrete-fern%C3%A1ndez (Recuperado. El 18 de diciembre 2021).

Novoa I. Venegas L. (2020). *Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional.* Universidad de Chile. https://repositorio.uchile.cl/bitstream/handle/2250/176344/Herramientas-del-convenio-de-Budapest-sobre-ciberdelincuencia-y-su-adecuacion-a-la-legislacion-nacional.pdf?sequence=1&isAllowed=y (Recuperado. El 12 de enero 2022).

OAS. (2019). *Combatir la violencia en línea un llamado a la protección contra las mujeres*. https://www.oas.org/es/sms/cicte/docs/20191125-ESP-White-Paper-7-VIOLENCE-AGAINST-WOMEN.pdf (Recuperado. El 22 de enero 2022).

Organización Mundial de la Salud. (2002). *Violencia Y Salud Mental.* Pág. (3). https://www.uv.mx/psicologia/files/2014/11/Violencia-y-Salud-Mental-OMS.pdf (Recuperado. El 25 de diciembre 2021).

Ortega R, Elipe P, Mora. J. Genta L. Brighi A, Guarini A, et al. (2012). *The emotional impact of acoso escolar and cyberbullying on victims: a European cross-national study*. Aggress Behav.; Págs. (38: 342-56). (Recuperado. El 18 de enero 2022).

Pazmiño, P. (2010). *El impacto de las redes sociales y el internet en la formación de los jóvenes de la Universidad Politécnica Salesiana.* Universidad Politecnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/2618/1/Tesis%20Impacto%20de%20las%20Redes%20Sociales%20y%20el%20Internet.pdf (Recuperado. El 28 de diciembre 2021).

PRC. (2018). *Online Harassment & Cyberstalking. Retrieved November 5, 2019, from Privacy Rights Clearinghouse* website: https://privacyrights.org/consumer-guides/online-harassment-cyberstalking (Recuperado. El 4 de Enero 2022).

Reyna-Villasmil. Et. (2018). *Características del ciberacoso y psicopatología de las víctimas.* Fucsalud Pág. (190). https://www.fucsalud.edu.co/sites/default/files/2018-11/Art-10.pdf (Recuperado. El 13 de diciembre 2021).

Sampasa. H. et. al. (2014). *Breakfast skipping is associated with cyberbullying and school bullying victimization. A school-based cross-sectional study.* Pubmed https://pubmed.ncbi.nlm.nih.gov/24746660/ (Recuperado. El 8 de enero 2022).

Sánchez, L y otros. (2016). *Los adolescentes y el ciberacoso.* Plan Municipal de Drogodependencias. Pag. (30-31).

http://www.fundacioncsz.org/ArchivosPublicaci ones/292.pdf (Recuperado. El 14 de enero 2022).

Sierra M. (S.F*). Las redes sociales, sus riesgos y la manera de protegerse*. Ces. https://repository.ces.edu.co/bitstream/handle/10946/1970/Articulo%20de%20grado%20de%20las%20redes%20sociales%20aprobado.pdf;jsessionid=92D6A7171315C6387D26A661DF3E7113?sequence=1 (Recuperado. El 10 de marzo 2022).

Sullivan, K., Cleary, M. & Sullivan, G. (2010). Bullying en la enseñanza secundaria. El acoso escolar: cómo se presenta y cómo afrontarlo. CEAC. Pág. (116). https://books.google.com.ec/books?id=NHSCoaF8kqwC&printsec=frontcover&hl=es#v=onepage&q&f=false. (Recuperado. El 12 de marzo 2022).

Torre, Y. et. al. (2018). *Características del ciberacoso y psicopatología de las víctimas.* Fucsalud. Pág. (193). https://www.fucsalud.edu.co/sites/default/files/2018-11/Art-10.pdf. (Recuperado. El 10 de noviembre de 2021).

Trujano P. et. al. 2009. *Violencia en internet: nuevas víctimas, nuevos retos*. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1729-48272009000100002 (Recuperado. El 18 de diciembre 2021).

UNICEF. (2002). *Violencia Y Salud Mental.* OMS. https://www.uv.mx/psicologia/files/2014/11/Violencia-y-Salud-Mental-OMS.pdf

Urueña. A. y colaboradores Ferrari. D. Valdecasa. E. 2011. *Estudio Las Redes Sociales en Internet.* Observatorio Nacional de la Telecomunicaciones ONTSI. Fondo Europeo de Desarrollo Regional. Pág. (82) https://www.ontsi.es//sites/ontsi/files/ redes_sociales-documento_0.pdf (Recuperado. El 10 de diciembre 2021).

Vidal, F. (2008). *Los nuevos aceleradores de la violencia remodernizada*. Universidad Pontificia Comillas de Madrid. Págs. 17-20.

https://www.torrossa.com/es/ resources/an/2488430 (Recuperado. El 11 de enero 2022).

Marín-Cortés. A. Et. Al. 2019, Factores De Riesgo Y Factores Protectores Relacionados Con El Ciberbullying Entre Adolescentes: Una Revisión Sistemática. Papeles del psicólogo. Pág. (111). http://www.papelesdelpsicologo.es/pdf/2899.pdf (Recuperado. El 9 de marzo 2022).