FIPCAEC (Edición 30) Vol. 6, No 4
Octubre 2021, pp. 336-363

ISSN: 2588-090X

DOI: https://doi.org/10.23857/fipcaec.v6i4.485

Derechos fundamentales y criminalidad cibernética en niños, niñas y adolescentes: análisis para la no indefensión de la víctima

Fundamental rights and cyber criminality in children, girls and adolescents: analysis for the non-indefension of the victim

Direitos fundamentais e crimes cibernéticos em crianças e adolescentes: uma análise para a indefesa da vítima

Diana Catalina Toledo-Verdugo [I]
diana.toledo.90@est.ucacue.edu.ec
https://orcid.org/0000-0003-1912-5738

Fernando Esteban Ochoa-Rodríguez [II]
fernando.ochoa@ucacue.edu.ec
https://orcid.org/0000-0002-4768-3828

Correspondencia: diana.toledo.90@est.ucacue.edu.ec

*** Recepción:** 25/08/2021 *** Aceptación:** 28/09/2021 ***Publicación**: 29/10/2021

1. Abogada, estudiante de la Maestría en Derecho Constitucional con Mención en Derecho Procesal Constitucional, Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.
2. Docente de la Maestría en Derecho Constitucional con Mención en Derecho Procesal Constitucional, Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

En el contexto de la virtualidad acelerada desde el inicio de siglo e intensificada indiscriminadamente en el contexto de la pandemia, resulta obstinado decir que las relaciones sociales se limitan a la materialidad física conocida hasta el pasado siglo e incluso la pasada década. Este nuevo espacio social, ha generado que fenómenos humanos se transmitan a este escenario, fenómenos positivos, pero a la par se constituye en el génesis de una continua producción de problemas que afectan derechos constitucionales. Así, la delincuencia, ha observado en el espacio de la virtualidad, un escenario apto para perpetrar, todo tipo de ilícitos; aún más, cuando se tiene como víctimas de estos ciber delitos a niños, niñas y adolescentes.

La presente investigación, luego de brindar el soporte jurídico y doctrinario en torno a ciberdelincuencia; ha podido dilucidar, el no actuar oportuno del Estado en la prevención, investigación, sanción y reparación, por este tipo de delitos. El objetivo es dar a conocer tres problemas que se verifican, siendo estos, la revictimización, la dificultad probatoria, y la desidia estatal. Se propone una adecuación normativa al Art. 454 número 6 del COIP, a efectos de desformalizar moderadamente la prueba en este tipo de delitos; ello, cuando las víctimas son niños, niñas y adolescentes. Se propone la suscripción por parte del Ecuador al Convenio de Budapest, principal instrumento internacional para la prevención y combate al cibercrimen. La investigación fue no experimental, de tipo mixta con énfasis en lo cualitativo, los métodos utilizados fueron, inductivo-deductivo.

Palabras clave: Derecho Constitucional; ciberdelitos; responsabilidad estatal grupo de atención prioritaria, reparación.

Abstract

Today, in the context of virtuality, accelerated since the beginning of the century and intensified indiscriminately in the context of the pandemic, it is stubborn to say that social relations are limited to physical materiality known until the last century, and even the past decade. This new social space has generated that human phenomena are transmitted to this scenario, positive phenomena, but at the same time, it constitutes the genesis of a continuous production of problems that affect constitutional rights. Thus, crime, has observed in the space of virtuality, a

scenario, apt to perpetrate, all kinds of illicit; even more so, when children and adolescents are the victims of these cybercrimes.

The present investigation, after providing legal and doctrinal support on cybercrime; It has been able to elucidate the failure of the State to act opportunely in the prevention, investigation, punishment and reparation for this type of crime. The objective is to publicize three problems that are verified, these being revictimization, evidentiary difficulty, and state laziness. A normative adaptation to Article 454 number 6 of the COIP is proposed, in order to moderately distort the evidence in this type of crime; this, when the victims are children and adolescents. It is proposed that Ecuador subscribe to the Budapest Convention, the main international instrument for preventing and combating cybercrime. The research was non-experimental, of a mixed type with emphasis on the qualitative, the methods used were inductive-deductive.

Keywords: Constitutional Law; cybercrime; State responsibility priority care group, repair.

Resumo

No contexto da virtualidade acelerada desde o início do século e intensificada indiscriminadamente no contexto da pandemia, é teimoso dizer que as relações sociais se limitam à materialidade física conhecida até o século passado e mesmo a década passada. Este novo espaço social, tem gerado que se transmitam a este cenário fenômenos humanos, fenômenos positivos, mas ao mesmo tempo constitui a gênese de uma produção contínua de problemas que afetam os direitos constitucionais. Assim, o crime, tem observado no espaço da virtualidade, um cenário adequado para perpetrar todo tipo de crime; ainda mais quando crianças e adolescentes são vítimas desses crimes cibernéticos.

A presente investigação, após fornecer suporte jurídico e doutrinário sobre crimes cibernéticos; Conseguiu elucidar a omissão do Estado em atuar oportunamente na prevenção, investigação, punição e reparação deste tipo de delito. O objetivo é divulgar três problemas verificados, sendo eles a revitimização, a dificuldade probatória e a preguiça do estado. É proposta uma adaptação normativa ao artigo 454.º n.º 6 do COIP, de forma a distorcer moderadamente as provas neste tipo de crime; isso, quando as vítimas são crianças e adolescentes. Propõe-se que o Equador subscreva a Convenção de Budapeste, o principal instrumento internacional de prevenção e

combate ao crime cibernético. A pesquisa foi não experimental, do tipo misto com ênfase na qualitativa, os métodos utilizados foram indutivo-dedutivo.

Palavras-chave: Direito Constitucional; cibercrime; Grupo de cuidados prioritários de responsabilidade estatal, reparo.

Introducción

Alrededor de la criminalidad cibernética, como relativamente nueva modalidad de la cual se derivan un sinnúmero de conductas delictivas, aún más cuando tiene como víctimas a niños, niñas y adolescentes; se suma la precariedad de los sistemas judiciales actuales, cuyo proceder se enmarca en formas comisivas tradicionales que van quedando obsoletas ante estas nuevas formas de actos delictivos; que afectan considerablemente los derechos constitucionales del grupo de atención prioritaria y trato preferente indicado.

En nuestro país Ecuador, según el Instituto Nacional de Estadísticas y Censos se considera que 15. 934. 522 de personas, (el 92 % de la población mayor a 5 años), cuenta con teléfonos celulares y también redes sociales, y de este segmento, el mayor uso de estas tecnologías de comunicación, se encuentra en las edades comprendidas entre los 16 y 44 años de edad; de ahí la trascendencia en la regulación en cuanto a los ataques cibernéticos a niños, niñas y adolescentes.

Cierta parte de la academia y doctrina ha sabido mantener una posición radical, al manifestar la necesidad de un sistema penal de nueva velocidad; ello, en cuanto a casos de ciberdelincuencia digital que lesionan los bienes jurídicos protegidos, lesionando además la estructura social de manera severa. "(…) Debe tenerse en cuenta que la tecnología siempre va delante de los gobiernos en una carrera desigual, y ello es así, aunque la sociedad de que se trate sea de avanzada (…)" (Dupuy & Kiefer, 2018).

La criminalidad cibernética se materializa en conductas como el cyberbullying, grooming, sexting, entre otras formas; cada una de ellas con sus marcadas diferencias, pero que, en forma global tienen como génesis o punto de partida el abuso de los medios virtuales para la perpetración de delitos; y, en el caso en particular son niños, niñas y adolescentes, quienes terminan siendo objeto de manipulación por parte de su agresor, en abuso a su vulnerabilidad, y su falta de desarrollo.

Es esta vulnerabilidad e indefensión de los heteroadministrados, además, de las macabras secuelas que produce el cometimiento de estos ilícitos penales, viene marcado por la lentitud estatal, en cuanto a tomar acciones preventivas para el no cometimiento del delito, debemos tener presente; claro está, que la hiperinflación punitiva no es, per se, la panacea para erradicar los ataques cibernéticos en menores de edad; empero, que estén regulados los tipos penales, ayuda en la investigación, sanción y reparación; tal es así que en la reciente aprobación de la Ley Orgánica Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos, normativa de reciente data que entró en vigencia el 30 de agosto del 2021; mediante publicación en el Registro Oficial Nro. 526; se contempla tanto la reforma de algunos tipos penales, así como, la incorporación de nuevos tipos penales atinentes a los ciberdelitos cometidos en contra de niños, niñas y adolescentes; que serán analizados en lo posterior.

Debemos tener presente que los niños, niñas y adolescentes, son considerados constitucionalmente como un grupo vulnerable de atención prioritaria; de hecho, así lo consagra el Art. 35 de la Carta Iusfundamental; en concordancia con el Art. 44; y 66 ejusdem; siendo este último el artículo que contempla el bien jurídico de la integridad, tanto en su esfera, física, psicológica, moral y sexual; a más de ello, es de advertir que también convencionalmente este grupo de atención prioritaria, se encuentra cobijado por la Convención sobre los Derechos del Niño; instrumento internacional aprobado por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989, y que brinda protección y tutela a los niños, niñas y adolescentes frente a todo tipo de abusos; endilgando a los Estados la responsabilidad de cuidar de su integridad; de hecho el Art. 19 del prenombrado instrumento internacional; contempla justamente, el deber estatal en cuanto a adoptar todas las medidas, sean de índole administrativa, legislativa, económicas, judiciales, etc., apropiadas para la protección del grupo vulnerable frente a toda forma de violencia, entre las cuales obviamente se incorpora la violencia de carácter sexual; la que primordialmente se analiza en el presente trabajo, con el cometimiento de delitos cibernéticos.

Se presenta como objetivo, el brindar un soporte doctrinario, constitucional y legal sobre los ciberdelitos en el Ecuador, en cuanto tienen como víctimas a niños, niñas y adolescentes; así, analizar la reciente normativa expedida en el país, buscando además poner en evidencia, tres

problemas existentes en cuanto a la prevención, investigación, sanción y reparación por este tipo de conductas ilícitas que afectan derechos constitucionales, siendo estos, la revictimización, la dificultad probatoria y la desidia estatal; realizando propuestas de adecuación normativa, así como cabe la interrogante ¿cómo exhortar al Estado a tomar medidas más oportunas para el combate a la ciberdelincuencia, en cuanto a campañas preventivas y suscripción de convenios internacionales?; el trabajo cuenta además con entrevistas a dos expertos en el área informática y que cuentan con experiencia en ciberdelincuencia.

Marco Teórico

Naturaleza del Entorno Informático como medio para cometer delitos.

Tenemos como antecedentes normativos, que regulaban las conductas ilícitas teniendo como herramienta el campo informático los siguientes: "En primer lugar se estableció en EEUU la Crime Control Act de 1984, seguida de la Computer Fraud and Abuso Act de 1986 que incluía cinco grupos de ilícitos informáticos. En Alemania en el marco de la segunda ley de lucha contra la criminalidad económica de 15 de mayo de 1986, se introduce la regulación relativa a la conocida como Computer Kriminalität. La seguridad informática se formalizó en Francia mediante la llamada ley Godfrain de 5 de enero de 1988, después incorporada al nuevo Código penal francés. En Italia la ley de 23 de diciembre de 1993 (n. 547) ha supuesto la adaptación del Código penal italiano a la nueva criminalidad informática"(Mata y Martín, 2003)

Debemos entender en primer lugar lo que es un delito, así la doctrina define al delito como una acción típica, antijurídica, culpable y que cumple otros eventuales presupuestos de punibilidad (Roxin, 1997). Un concepto tradicional define al delito informático como, "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software" (Davara Rodríguez, 1990).

Una concepción moderna define al delito informático como; "aquel conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectan al funcionamiento de los sistemas informáticos" (Salamea Carpio, 2013)

En la Cumbre de Madrid, sobre facturación electrónica llevada a cabo en abril del 2010; se calificó a la Ciberdelincuencia como "actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes o sistemas"; y se estableció tres tipos de actividades delictivas que comprende el cibercrimen. 1.- Formas tradicionales de delincuencia. 2.- Publicación de contenido ilegales a través de medios de comunicación electrónicos (ejemplo imágenes de abusos sexuales a menores de edad). 3.- Delitos específicos de las redes electrónicas, por ejemplo, ataques contra los sistemas informáticos; hackeos, piratería, etc., (Salamea Carpio, 2013).

En el marco convencional, el 23 de noviembre del 2001, fue expedido el Convenio sobre la Ciberdelincuencia, conocido como "Convenio de Budapest"; el cual definió al sistema informático como todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran en ejecución de un programa, el tratamiento automatizado de datos. Así este convenio que entró en vigencia en julio 2004; se ha convertido, en un importante, marco normativo internacional, en la lucha contra la cibercriminalidad; pues pretende armonizar las leyes nacionales, establecer mecanismos de cooperación internacional y desarrollar técnicas de investigación para menoscabar el cometimiento de los delitos informáticos o cibercrímenes; como en el caso en estudio, aquellos delitos que son cometidos en contra de niños, niñas o adolescentes, delitos inclusive de naturaleza sexual.

Empero de la trascendencia de este instrumento internacional de Hard Law, es decir, de derecho duro y de cumplimiento obligatorio para los países suscriptores y que lo han ratificado; llama profundamente la atención que nuestro país el Ecuador no lo haya suscrito ni ratificado; haciendo notar una vez más, la desidia estatal, en cuanto al tratamiento adecuado para hacer frente a la cibercriminalidad; pues ante la carencia normativa de reglas que tipifiquen adecuadamente las conductas delictivas, y que, es más han sido promulgadas en este año, tampoco se ha suscrito, el primer convenio sobre cibercriminalidad y el más importante, pese a estar vigente desde el año 2004; situación preocupante y alarmante, pues el Art. 19 de la Convención sobre los derechos del Niño, obliga a los estados miembros a adoptar todo tipo de medidas en protección de este grupo prioritario y vulnerable; pero a más de ello la propia Carta Constitucional consagra como una obligación estatal, en el número 4 del artículo 46, en cuanto a niños, niñas y adolescentes; brindar:

> Protección y atención contra todo tipo de violencia, maltrato, explotación sexual o de cualquier otra índole, o contra la negligencia que provoque tales situaciones. (…) Las acciones y las penas por delitos contra la integridad sexual y reproductiva cuyas víctimas sean niñas, niños y adolescentes serán imprescriptibles.

Recordemos, que inclusive este artículo constitucional fue reformado a consecuencia de la consulta popular efectuada el 4 de febrero del 2018; cuando se aprobó la imprescriptibilidad de los delitos sexuales cometidos en contra de niños, niñas o adolescentes; que engloba tanto la pena como la acción penal.

Un punto importante a tener en cuenta en la cibercriminalidad cometida en contra del grupo vulnerable indicado, es que,

> (…) La doctrina ha clasificado los delitos informáticos según el objeto de protección. Si el bien jurídico afectado se relaciona con los datos o información automatizada a la que se accede de modo no autorizado, los llama **propios**. En cambio, son **impropios** aquellos en los que la informática es utilizada como medio para la comisión de un delito distinto de aquel de acceso no autorizado (Alajia, de la Luca, & Slokar, 2014) (Sic) (énfasis me pertenece).

Así, por ejemplo, tenemos que en la mayoría de los casos de delitos cibernéticos cometidos en contra de niños niñas o adolescentes; existe una finalidad, de cometimiento de otros delitos, por ello, es que en su mayoría son impropios.

Tipos de ciberdelitos cometidos en contra de niños, niñas o adolescentes.

Si volvemos nuestra mirada en el tiempo, podremos identificar que la problemática existente hace veinte años atrás en hogares, oficinas, relaciones de amistad y otros ámbitos, giraban en torno a aspectos muy lejanos a la tecnología, pues en aquel entonces, resultaba impensable, el tener que exigir al Estado que incluya en su legislación, tipificación referente a delitos que se perpetren a través del internet.

Son los acelerados avances tecnológicos los que han introducido nuevas exposiciones de las personas y con ello riesgos en la sociedad actual. Las nuevas tecnologías, llegaron para mudar de forma radical el comportamiento de toda una sociedad, la que se ha visto obligada a caminar de la mano con su avance, sin que sea una opción el replegarse; pudiéndose identificar que, si bien se

ha simplificado y facilitado la comunicación, rompiendo incluso barreras fronterizas, una vez inmersos en un mundo globalizado, no solo podemos enfocarnos en los beneficios que otorga; sino por el contrario, estar alertas a los nuevos riesgos de la sociedad, debiendo el estado esforzarse en adaptar en su normativa aquellas actividades delictivas que vayan relacionadas con el uso de tecnología informática.

Considerar que inclusive nuestras legislaciones resultan estar en pañales al respecto; y, lo que hoy se considera un logro, en nuestro ordenamiento jurídico, muy pronto quedará obsoleto, pues, el acelerado avance de aquellas formas de delinquir a través de la red, amerita no solamente visualizar el aspecto punitivo, sino por el contrario contrarrestarlo desde una óptica de prevención a temprana edad y a través de la implementación de políticas estatales en el marco inclusive convencional.

Tipos de Acosos Cibernéticos

Como tipos de acosos cibernéticos, son considerados: El Grooming, Ciberbullying, Sexting, Happy Slapping.

Grooming: comprende el contacto, mediante canales informáticos, con menores de edad, para conseguir finalidades de índole sexual.

Ciberbullying: Se describe como abuso psicológico entre iguales o de edad similar. En este caso, a diferencia con el bullying, es el medio a través del cual se produce el acoso, puesto que, en el ciberbullying, se utilizan nuevas tecnologías de la información y comunicación (NTIC).

Sexting: Se define como el envío de contenidos eróticos o pornografía entre dispositivos móviles, en la mayoría de las ocasiones, aunque también pueden utilizarse otras vías.

Happy Slapping: Se traduce al español como "bofetada feliz", es un fenómeno en el que un grupo de personas, normalmente adolescentes, buscan a otra, sea conocida o no para propiciarle una paliza (golpes, patadas, bofetadas); además de toda clase de insultos. Dichos actos violentos no acaban aquí, dado que el objetivo último es grabar o fotografiar lo que se le hace a la víctima seleccionada…para subirlo a la red o enviar a sus contactos. Cabe destacar que una de las características es la ausencia de provocación de la víctima. (Vecina Navarro & Molina del Peral, 2015, págs. 47, 57)

Conceptualización, aproximaciones doctrinarias, legales y bienes jurídicos tutelados.

Los Derechos fundamentales, aquellos, propios de la dignidad humana, son materializados y reconocidos en la Constitución, entonces pasan a nominarse, derechos constitucionales, la doctrina al respecto nos refiere que:

> Los derechos fundamentales garantizados por la Ley fundamental aparecen como resultado del reconocimiento de la inalienabilidad de los derechos del hombre, los cuales, por su lado, tienen su fundamento en la inviolabilidad de la dignidad humana. Con ello los derechos fundamentales están cimentados metapositivamente y ubicados en un determinado contexto de fundamentación (…) He aquí el sistema dual de los derechos constitucionales, por un lado, derechos subjetivos y, por el otro, normas objetivas, esto es, normas constitucionales con contenido axiológico que irradian sus efectos a toda la normativa del Ordenamiento jurídico, tanto la que rige las relaciones sujeto-poder público como la que regula las derivaciones de la autonomía de la voluntad perteneciente al Derecho Privado, lo cual constituye la esencia del Estado constitucional de derechos y justicia (Zavala Egas, 2010).

En nuestro país, existen tipificadas, ciertas conductas como infracciones penales delictuales y contravencionales, que pueden ser cometidas por medios telemáticos; es decir, son propiamente ciber infracciones; y que, de hecho al momento, con las reformas al Código Orgánico Integral Penal, mediante la Ley Orgánica Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos; se ha incorporado al catálogo de delitos, nuevos tipos penales, algunos de ellos con énfasis en cuanto a tener como víctimas a niños, niñas o adolescentes; mientras que otros tipos penales han sido reformados.

Es menester entonces, hacer alusión a los principales tipos penales, que contempla nuestra legislación en su código sustantivo penal, a efectos de ilustrar, sobre las conductas que el legislador ha considerado lesionan a los bienes jurídicos tutelados, en el presente caso con respecto a niños, niñas o adolescentes; bienes jurídicos que se encuentran contenidos en el Art. 66 de nuestra Constitución y consagrados en los siguientes números:

> 1. El derecho a la inviolabilidad de la vida. 2. Derecho a una vida digna (que asegure la salud, alimentación y nutrición, agua potable, vivienda, saneamiento ambiental,

educación, trabajo, empleo, descanso y ocio, cultura física, vestido, seguridad social y otros servicios sociales necesarios); 3. El derecho a la integridad personal, que incluye, a integridad, física psíquica, moral y sexual, una vida libre de violencia, en el ámbito público o privado y prohibición de tortura; 9. El derecho a tomar decisiones libres, informadas, voluntarias y responsables sobre su sexualidad, y su vida y orientación sexual. 18. El Derecho al honor, buen nombre y la imagen. 19. Derecho a la Protección de Datos de Carácter personal; 20. Derecho a la intimidad personal y familiar. 21. Inviolabilidad de secreto y correspondencia, física y virtual.

Estos son los derechos que se encuentran siendo consagrados en la Carta Ius fundamental de Montecristi, los mismos que buscan ser tutelados por parte del Estado, y que, para el derecho penal se transforman en bienes jurídicos que merecen ser protegidos; en tal virtud; y, en cuanto a los principales tipos penales que admiten modalidad de ciber crimen, teniendo como víctimas a niños, niñas y adolescentes, vamos a describirlos en forma concisa.

Pornografía con utilización de niñas, niños o adolescentes. Tipo penal descrito en el Art. 103 del COIP; y que fue reformado con la Ley *para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos;* así tenemos que en la descripción típica se indica que la persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tenga su origen en el extranjero o sea desconocido, tendrá una pena privativa de libertad de trece a dieciséis años.

La doctrina en cuanto a este tipo penal refiere que este género delictivo ha sido el que más aprovechó de la utilización abusiva de la red informática en contra de niños, niñas y adolescentes; que afecta gravemente su indemnidad sexual, y a la par deja profundas e indelebles huellas en sus inocentes psiquis. (Aboso & Zapata, 2006)

Hostigamiento. Este tipo penal, es conocido doctrinariamente como el Ciberbullyng. Constante en el numeral 2 del Art. 154 del COIP; tipo penal nuevo en nuestra legislación, incorporado, mediante las reformas a las cuales se hace alusión en el presente trabajo; es decir, de reciente data en lo medular y atinente al tema que nos ocupa tenemos en la descripción típica a la persona natural o jurídica que, por sí misma o por terceros o a través de cualquier medio tecnológico o

digital, moleste, perturbe a angustie de forma insistente o reiterada a otra, tendrá una pena privativa de la libertad de seis meses a un año, siempre que el sujeto activo de la infracción busque cercanía con la víctima para poder causarle daño a su integridad física o sexual. Segundo inciso. Cuando la víctima sea menor de dieciocho años de edad, o persona con discapacidad o cuando la persona no pueda comprender el significado del hecho o por cualquier causa no pueda resistirlo, el autor será sancionado con una pena privativa de libertad de uno a tres años.

Contravenciones de acoso escolar y académico. Se hace alusión a las infracciones contempladas en el numeral 3 del Art. 154; igualmente de última data; con las reformas mentadas al COIP. Es de indicar que las infracciones penales pueden ser delitos, pero también contravenciones, así tenemos que han sido tipificadas las siguientes contravenciones:

Acoso académico: Se entiende por acoso académico a toda conducta negativa, intencional, metódica y sistemática de agresión, intimidación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza, incitación a la violencia, hostigamiento o cualquier forma de maltrato psicológico, verbal, físico que, de forma directa o indirecta, dentro o fuera del establecimiento educativo, se dé por parte de un docente, autoridad o con quienes la víctima o víctimas mantienen una relación de poder asimétrica que, en forma individual o colectiva, atenten en contra de una o varias personas, por cualquier medio incluyendo a través de las tecnologías de la información y comunicación.

Acoso escolar entre pares: Cuando las mismas conductas descritas para el acoso académico se produzcan entre estudiantes niñas, niños y adolescentes, se aplicarán las medidas socioeducativas no privativas de libertad correspondientes y el tratamiento especializado reconocido en la ley de la materia, garantizando los derechos y protección especial de niñas, niños y adolescentes. Es decir, en este último caso será el juzgador especializado en niños y adolescentes infractores quien deberá sancionar la conducta en base al Código de la Niñez y Adolescencia.

Acoso sexual. Este tipo penal, si bien es cierto existía ya en el COIP en el Art. 166; la ley reformatoria de marras, ha incorporado un nuevo concepto a dicha descripción típica; un nuevo concepto muy importante para el presente análisis, pues aparte de describir la conducta constitutiva del tipo penal de Acoso Sexual, define al Ciber Acoso.

Así tenemos que el legislador en lo medular en cuanto al acoso sexual se refiere a la persona que solicite algún acto de naturaleza sexual, para si o para un tercero, prevaliéndose de situación de autoridad laboral, docente, religiosa o similar, sea tutora o tutor, curadora o curador, ministros de culto, profesional de la educación o de la salud, personal responsable en la atención y cuidado del paciente o que mantenga vínculo familiar o cualquier otra forma que implique subordinación de la víctima con la amenaza de causar a la víctima o a un tercero un mal relacionado con las legítimas expectativas que pueda tener en el ámbito de dicha relación de subordinación, esta conducta tiene una pena privativa de libertad de uno a cinco años.

Por otra parte se considera **Ciberacoso sexual** cuando la conducta descrita como acoso sexual se realice utilizando cualquiera de las tecnologías de la información y comunicación, medios tecnológicos, electrónicos o digitales, pero a más de ello cuando la víctima sea menor de dieciocho años de edad, o persona con discapacidad o cuando la persona no pueda comprender el significado del hecho o por cualquier causa no pueda resistirlo, el autor tendrá una pena privativa de libertad de tres a cinco años.

Es importante tambien indicar que el tipo penal, para efectos del cuantum punitivo, ha establecido por ejemplo que, si la víctima ha tenido conductas autolesivas o afectaciones en su conducta consecuencia del ciber acoso, el agresor deberá ser penado con e máximo de la sanción punitiva. Nos dice la doctrina que, en una segunda fase del ciberacoso, estaría de manifiesto la confusión, el acoso y el derribo, siendo esta la que mayor hostigamiento produce hacia el acosado. La aparición de daños psicológicos graves, acompañados de sintomatología física sería la tercera fase que conforma el proceso; y, una cuarta y última fase que es el desenlace final del proceso, en el cual se desembocaría inclusive en consecuencias fatídicas, como el suicidio (Vecina Navarro & Molina del Peral, 2015)

Corrupción de niñas, niños y adolescentes. Este tipo penal tambien ha sido reformado en el COIP, y se encuentra establecido en el Art. 169. Se hace alusión al nuevo inciso incorporado, que atañe al caso en estudio; pues el mismo refiere a la persona que permita el acceso o exposición de niñas, niños o adolescentes de forma intencionada a contenido nocivo sexualizado, violento o que llame a cometer actos de odio será sancionada con pena prisión de uno a tres años. En este punto debemos recalcar que el acceso o exposición del grupo vulnerable a contenidos nocivos sexualizados, o violentos, se lo puede hacer por cualquier medio entre ellos, claro está los medios

telemáticos o virtuales, en este caso, se utiliza el medio telemático como una herramienta para la perpetración del delito, de ahí que es un ciberdelito impropio.

Abuso sexual y violación, los artículos 170 y 171 del COIP respectivamente. Si bien estos tipos penales, han estado ya descritos como conductas delictivas en el COIP; en las reformas publicadas el 30 de agosto del 2021; se incorpora para los dos tipos penales algo novedoso, y aquello es justamente que se sancionará con el máximo de las penas establecidas en cada tipo penal, cuando dicho abuso sexual o violación fuese grabada o transmitida en vivo de manera intencional por la persona agresora, por cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación (TICs). En este punto es de resaltar que el uso de medios telemáticos convierte al tipo penal sea violación u abuso sexual, en un tipo penal agravado, cuya sanción es el máximo de la sanción punitiva.

Extorsión sexual. Esta figura penal, el el código sustantivo penal consta en el numeral 1 del Art. 172, e igualmente ha sido incorporada con la Ley reformatoria al COIP en fecha 30 de agosto del 2021; el tipo penal que también puede ser cometido por medios telemáticos, describe a la persona que, mediante el uso de violencia, amenazas o chantaje induzca, incite u obligue a otra y exhibir su cuerpo desnudo, semidesnudo o en actitudes sexuales, con el propósito, de obtener un provecho personal o para un tercero, ya sea de carácter sexual o de cualquier otro tipo, será sancionado con pena privativa de libertad de tres a cinco años.

Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos. Este tipo penal se encuentra en el Art. 173 del COIP; y describe el conocido **Grooming**. El tipo penal describe, 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, tendrá prisión de uno a tres años.

El origen del término “grooming” surge de la tradición anglosajona para referirse a este fenómeno. Se han usado otras expresiones, por ejemplo “solicitation of children for sexual purposes” (solicitud/propuesta/aproximación a menores con propósitos sexuales) que surge del Convenio de Lanzarote, o “Soliciting”, utilizado por la directiva 2011/93/UE de la Unión Europea (Carolina, 2020, pág. 13); sin embargo, existe un relativo consenso, a pesar de las

múltiples denominaciones, del empleo de Grooming o Child-grooming para enfrentar conceptualmente este fenómeno. Dentro de la doctrina, hay quienes entienden al "Grooming" como un tipo de acoso, equiparándolo a un *cyberacoso* de menores, dejando diletante la parte sexual intrínseca dentro del childgrooming, y también hay quienes lo intentan figurar como el *acceso a niños con fines sexuales, a través de las tecnologías de la información y comunicación*.

El significado pertinente de "Groom" se refiere a "to prepare for a particular job", es decir, preparar a alguien para una labor/función/propósito. Lo que nos lleva a mencionar que nos encontramos frente a un fenómeno cuyo desarrollo se presenta como un proceso.

Para Ana Salter, el grooming es la *seducción emocional;* mientras que para Sylvia Kierkegaard, es una "estrategia utilizada por potenciales abusadores para seducir a los niños, y conseguir que realicen conductas sexuales" (Salter & kierkegaard) en (Granja, Internet y Pederastas , 2020, pág. 16)

Las características del grooming, varían según la configuración de su concepto, que gira en torno a dos variantes: aquellas que se forman alrededor de la idea de *seducción,* o cuando la constitución de su concepto se erige alrededor de la idea de pedofilia. Es decir, la primera concebida como táctica de seducción dirigida a la realización de conductas sexuales por parte del menor; mientras que por la articulación en base a la pedofilia se lo concibe como *"los pasos que realizan los pedófilos para atrapar a sus víctimas".* Sin embargo, dentro lo aceptado en la academia gira en torno a los conceptos de grooming en tanto "*proceso conducente a ganarse la confianza de la víctima",* donde se lo concibe como aquel "proceso a través del cual un posible abusador entabla amistad con el intento de ganarse su confianza, con el fin de que el niño consienta actividades abusivas" (GuillesPie, 2020, pág. 17)

También se lo define como la "estrategia empleada por los abusadores para manipular al niño, de manera que el abusador tiene un control total sobre la víctima. Proceso donde el abusador vence gradualmente la resistencia de la víctima mediante una secuencia de actos de manipulación psicológica, misma que se usa para silenciar al menor una vez producido el abuso". Es así que, el grooming en tanto proceso, está directamente relacionado con el abuso sexual, siendo esta la fase sexual o fase final del grooming. (Villacampa, Internet y Pederastas Pedro Granja, 2020, pág. 17)

Cualquier modalidad planificada de *grooming* incluye, probablemente, varias fases. Es razonable pensar en la generación de un lazo de amistad con el menor, frecuentemente, fingiendo ser un

niño o una niña. Luego, la obtención de información del menor, preparando la fase de afectación. Una etapa que incluye la seducción, procurando conductas con significado sexual y quizá, finalmente, la extorsión para hacerse de pornografía o lograr contacto físico prohibido. Un complejo de conductas equiparable, en cierta forma, a la descripción realizada para los delitos informáticos en sentido estricto o propio, donde en todo caso la seducción en busca de ciertas conductas se equipara al acceso a los datos en los delitos propiamente informáticos (Alajia, de la Luca, & Slokar, 2014).

Es así que, dentro del grooming y todos aquellos con finalidad sexual en niños, niñas o adolescentes; como bien jurídico primordial se protege la *Indemnidad Sexual*, entendida como aquella intangibilidad en el normal desarrollo y formación de la vida sexual, y su derecho a no sufrir daño en aquella esfera. Debiéndose entender que su protección tiene dos dimensiones, una particular y una genérica, pues se protege la indemnidad sexual particular relativo al hecho actual, y se protege también -en tanto delito de peligro abstracto/hipotético- como bien jurídico colectivo, que es la *infancia en general.* (Granja, 2020)

La mayoría de legislaciones que tipifican y reprimen el child-grooming, "lo conciben como delito de resultado, lo cual es un error en tanto solo existe delito cuando el pederasta solicita el encuentro físico con el niño, lo que se entendería como lícito que un adulto contacte a un menor y mantenga un largo cruce de conversaciones eróticas o sexuales" (Granja, 2020)

Al igual que en la legislación peruana, siguiendo el principio de legalidad, no podríamos sancionar a un adulto, mientras "no proponga concertar un encuentro" tampoco cabe castigo, en caso de petición de fotos, audios y videos, debido a un penoso vacío normativo. Alarmante es también considerar que las penas en nuestro país, para el grooming van de uno a tres años, lo que permite que el pederasta digital pueda solicitar la suspensión condicional de la pena, lo que profundiza la indefensión de la víctima (Pedro, 2020)

Entre el grooming y la pederastia, entendido este último como la atracción sexual de un adulto hacia un niño, la diferencia radica precisamente en el medio en el cual se desarrolla y perpetra cada uno, siendo que el grooming acontece a través de los medios tecnológicos, mientras que el segundo en un medio físico, con esta relación, se pretende aludir que, el perfil del adulto que está detrás de ambos tipos de acoso, es similar.

Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos. Igualmente, este es un tipo penal que ya se encuentra tipificado en el COIP en su Art. 174; y no ha merecido cambios, empero, igualmente se convierte en un ciberdelito impropio; en tanto, tiene como finalidad ofertar servicios sexuales, por medio de canales telemáticos; así, el legislador ha descrito esta conducta y tiene como autor a 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, estableciendo una pena privativa de libertad de siete a diez años.

Estos son los principales ciberdelitos que tenemos tipificados en nuestra legislación penal; es de hacer énfasis en que es reciente la incorporación al catálogo delictual de figuras como las ya descritas; lo que evidentemente, da cuenta de la lentitud y omisión estatal en cuanto a regular y tipificar en forma oportuna este tipo de conductas que afectan gravemente los derechos constitucionales de niños, niñas y adolescentes; así tambien es de tener claro, que el consentimiento de aquellos, para los delitos de índole sexual es irrelevante, de conformidad con lo previsto en el numeral 5 del Art. 175 del COIP.

Dificultades Estructurales para la Sanción de los Ciberdelitos cometidos en contra de niños, niñas o adolescentes.

Se ha podido verificar, al momento, los derechos fundamentales y constitucionales que se encuentran afectados con el cometimiento de los ciberdelitos en contra de niños, niñas y adolescentes, como grupo de atención prioritaria; así tambien se ha pasado revista por los principales tipos penales delictuales y contravencionales, en donde se describen las conductas típicas que, mediante el uso de medios telemáticos, afectan no solo la indemnidad sexual de este grupo vulnerable, sino a muchos otros derechos como la integridad física, psíquica, moral, la libertad, la vida, entre otros.

Sin embargo, se busca relievar, tres problemas, existentes en cuanto a la eficacia del actuar estatal, para prevenir, investigar, sancionar y reparar, las afectaciones generadas a consecuencia del cometimiento de ciberdelitos en contra de este grupo vulnerable; estos problemas tienen que ver primero, con circunstancias de revictimización a quienes han sido víctimas de estos ciberdelitos; en segundo lugar, con la dificultad probatoria para llegar a sentencias condenatorias en este tipo de delitos; y como tercer problema, la desidia y lentitud estatal, en la prevención y

legislación de este tipo de conductas que afectan gravemente a los derechos de niños, niñas y adolescentes.

Revictimización

Se puede definir a víctima como la persona que sufre violencia injusta en su persona o ataque a sus derechos (Torres, 1993). Por su parte el Código Orgánico Integral Penal, en su Art. 411 números 1 y 2 define a víctima en lo atinente al objeto de estudio, como la persona natural o jurídica que ha sufrido algún daño a un bien jurídico de manera directa o indirecta como consecuencia de la infracción. Así también en su numeral 2 indica que se considera víctima a quien ha sufrido agresión física, psicológica, sexual o cualquier tipo de daño o perjuicio de sus derechos por el cometimiento de una infracción penal.

Las Cien Reglas de Brasilia para el acceso a la justicia de personas que se encuentran en condición de vulnerabilidad, entre las cuales; huelga advertir, se encuentran los niños, niñas y adolescentes; reza en su regla diez que, se considera víctima toda persona física que ha sufrido un daño ocasionado por una infracción penal, incluida tanto la lesión física o psíquica, como el sufrimiento moral y el perjuicio económico. El término víctima también podrá incluir, en su caso, a la familia inmediata o a las personas que están a cargo de la víctima directa. (XIV Cumbre Judicial Iberoaméricana, 2008)

El Art. 78 de la Carta Constitucional consagra el derecho de las víctimas a no ser revictimizadas; entendido dicho proceso, como aquel en el que, luego de la victimización primaria, es decir, el acto generador de la vulneración, circunstancias externas, atinentes al sistema de justicia, hacen que la víctima, siga aumentando, el sufrimiento, dolor o afección por el hecho delictual que le fue perpetrado; y también se habla de una victimización tercearia, que tiene que ver con el comportamiento posterior de la víctima, por ejemplo sea para vengarse. (Lovatón Palacios, 2009).

Por su parte el Código Orgánico Integral Penal en su Art. 11 número 5 contempla como uno de los derechos de las víctimas no ser revictimizada, particularmente en la obtención y valoración de las pruebas, incluida su versión. Así el Reglamento del Sistema de Protección a Testigos y Víctimas, en su Art. 7, letra f indica, como uno de los derechos de las personas protegidas, en el caso la víctima; no ser revictimizadas, particularmente en la obtención y valoración de las

pruebas, incluida su declaración o testimonio; se las protegerá de cualquier amenaza u otras formas de intimidación o desprecio en su dignidad; para tal efecto, en la fase pre procesal y en las etapas procesales se contará con asistencia profesional adecuada y se podrán utilizar los medios tecnológicos pertinentes.

En cuanto a los ciberdelitos; empezando por la afectación psicológica de la cual son parte, además son víctimas de hostigamiento, son presas del miedo, angustia, y un sentimiento de amenaza constante, lo cual reduce su autoestima, seguridad y capacidad de defenderse; inclusive en múltiples casos, la víctima ha sentido empatía con su agresor, siendo este último quien ha generado en aquella sentimientos de compasión, pues el agresor, en sus primeros acercamientos a la víctima la trata de engatusar, haciéndole creer que es su amigo, en muchas ocasiones utiliza el victimismo, el chantaje, con la finalidad de obtener favores; siendo en este caso que, muchas de las ocasiones la víctima llega a generar un alto grado de dependencia emocional respecto de su agresor, generándose de esta forma una especie de primera etapa, que es la de un acoso sutil.

La revictimización o victimización secundaria de niños, niñas y adolescentes, se perpetra muchas veces por cuanto, en el actuar investigativo del delito se hace que la víctima repita o narre los acontecimientos traumáticos, más de una vez, lo que revive a cada momento los hechos traumáticos vividos; así, la víctima cuenta a sus familiares, a la policía, en fiscalía, ante los facultativos, a los investigadores, al fiscal del caso, y luego al Juez. Así nos dice la doctrina que en cuanto al actuar probatorio se hace a la víctima recrear una y otra vez el hecho de violencia, que convierte al proceso de búsqueda de justicia en una nueva victimización. (Lovatón Palacios, 2009)

Se propone, que en caso de los delitos cometidos en contra de niños, niñas o adolescentes, en la praxis investigativa, la víctima, solo narre una vez los hechos, y que aquello sea ya tomado como prueba; pues si bien es cierto el Art. 504 del COIP, refiere que la versión o testimonio de este grupo prioritario, debe ser tomado una vez; no está claro como una versión pudiese constituir prueba, lo que va en contra del Art. 454.6 in fine del COIP; el cual establece que jamás una versión puede ser considerada como prueba. Está contradicción y obscuridad normativa debe ser solucionada, vía una Resolución de la Corte Nacional o mediante una reforma legal al Art. 454.6 del COIP, estableciendo como regla excepcional, la valía de la versión como prueba en este tipo de delitos, siempre y cuando se garantice los derechos de los menores de edad pero tambien el

derecho a la defensa; así, se materializa la garantía normativa, consagrada en la Constitución en su Art. 84, la cual ordena la adecuación formal y material, por parte del legislador, de toda la legislación infra constitucional, a la Constitución.

Dificultad probatoria en ciberdelitos.

Otro aspecto de gran interés es el de la prueba; la misma que debe ser entendida como la demostración, con ayuda de los medios autorizados por la ley, de la exactitud de un hecho (Solar, 1978)

La actividad probatoria, en los ciberdelitos, reviste cierta complejidad, dada la propia naturaleza y modo de cometimiento de estos delitos, pues se utiliza a la red informática, como medio para la comisión de los ilícitos; resulta así, complicada la labor investigativa, dado que el autor se esconde frente a un monitor o una pantalla, y el delito lo puede cometer, desde diferentes lugares, en distintos momentos, muchas veces sin dejar huellas claras, o que brinden el convencimiento suficiente al juzgador para enervar el estado de inocencia de una persona.

En cuanto a los ciberdelitos; la novedad y diferencias fundamentales con los métodos tradicionales de ejecución del delito hacen de la investigación y prueba de estos hechos un campo singular. El rastreo de los procesos automatizados de datos resulta especialmente complejo. Igualmente, la reproducción de la prueba en el proceso oral, único momento procesal en el que resulta válida la realización de la prueba de cargo suficiente para un veredicto de culpabilidad. (Mata y Martín, 2003, pág. 24)

El entorno digital, con los nuevos avances en técnicas delincuenciales, implica muchas veces la ausencia de huellas palpables o visibles; y, en caso de que se llegasen a obtener, el problema se trasladaría a poder a determinar sobre quien recae la responsabilidad de la infracción, ya que los elementos que revisten a los delitos informáticos son el ocultamiento, el anonimato, la distancia, su clandestinidad, el lugar de su comisión, dentro o fuera del país, para poder determinar la legislación aplicable, lo que involucraría inclusive una cooperación internacional.

Metodología

De acuerdo con el estudio adoptado para este trabajo de investigación, la metodología fue basada en la modalidad de carácter no experimental, puesto que no se han manipulado variables. Se ha

desarrollado un tipo de investigación cualitativa que se complementa por un diseño documental – bibliográfico, debido a la recolección de datos extraídos de diversos textos, enfocado en el contenido escrito.

Para este trabajo de investigación se ha utilizado el método inductivo - deductivo. Por cuanto el método inductivo permite partir de aspectos, condiciones, análisis o resultados particulares para llegar a generalizaciones, es decir, de lo particular a lo general, por el contrario, el método deductivo parte de aspectos, condiciones, análisis o resultados generales para aplicarlos a situaciones particulares. (Salinas, 2013). Se ha utilizado además el método dogmático jurídico por cuanto tiene por objeto el ordenamiento sistemático de los conceptos jurídicos, en este caso del tema de los ciberdelitos.

Además, se aplicó una entrevista a dos peritos expertos en el área informática, a quienes se les ha entrevistado, con tres preguntas a través del instrumento cuestionario.

Resultados

Ingeniero Andrés David Paredes Pozo. C.I: 1713987988. Acreditación del Consejo de la Judicatura Nro. 1831931. Perito informático, audio video, en área de criminalística. (Paredes Pozo, 2021)

1.- ¿Qué tan común la ciberdelincuencia, tiene como víctimas a niños, niñas y adolescentes? Hoy en día tenemos muchas redes sociales, de entre ellas las más comunes, Facebook Twitter, tik tok e Instagram, el tik tok era para niños; en base a esto la delincuencia ha accedido a los adolescentes niños y niñas, ha aumentado el 88% el ciber acoso, a raíz de la pandemia, y con el confinamiento así, la ciberdelincuencia o ciberbullyn, tienen varias aristas, varias formas delictivas como el acoso, acceder a fotografías, violación a la intimidad, trata de personas e incluso violación. Ahora también la pornografía infantil en niños pues por la cultura y la falta de vigilancia paternal, no están reguladas las redes como en otros países.

2.- ¿Qué tan complejo es el proceso de investigación para dar con los autores de este tipo de delitos; y por qué? Hay varias maneras de disimular el cometimiento de estos delitos; para dar con una persona que acosa a un niño, niña o adolescente, se le busca el IP, es como decir la cédula de la computadora, pero actualmente la tecnología que la denominamos, la red obscura la "Deep web", permite que las IPS se cambien, tienen otra nomenclatura, eso complica al

investigador saber de qué computador salió el ataque. Existen programas como por ejemplo "Tor"; esto dificulta, a que criminalística pueda determinar a los autores, se puede hacer de poco a poco seguimiento de llamadas telefónicas, triangulaciones, así, la policía tiene unos equipos para este tipo de investigaciones.

3.- ¿De su experiencia como perito que interviene en audiencias, cuántos casos de ciberdelitos, en contra de niños, niñas o adolescentes, han merecido sentencia condenatoria? La cultura ecuatoriana no da mucha confianza en la justicia, esto hace que, este tipo de delitos no sean denunciados, el ciber acoso es de parte de terceros, es engorroso, los familiares, de los niños, niñas o adolescentes, no suelen denunciarlos, o en mitad del proceso abandonan las causas, esto no ha permitido que se lleguen a sentencias mayoritarias, de un 5% a un 21% de delincuencia se ha incrementado en estos dos años, y se conoce que solamente un 3% de la gente que denuncia llega al final del proceso. El momento de que uno se entere de este delito, lo que debe hacer es darles a los niños la confianza e inmediatamente denunciar a las autoridades, y llegar con el proceso hasta el final.

3.2.2.- Sargento de Policía, Julio Castro Zaruma. C.I: 1103504955. Perito acreditado por el Consejo de la Judicatura Nro. 231416. Experto en criminalística, área de informática. (Castro Zaruma, 2021)

1.- ¿Qué tan común la ciberdelincuencia, tiene como víctimas a niños, niñas y adolescentes? Hoy es día, es muy común encontrar estos delitos por la ingenuidad de los menores de edad, aunque no están exentos los adultos, hay muchos menores de edad llamados la atención en las redes sociales para sacar provecho de fotografías, de uso pornográfico, como también para hacer cosas como robar. De las redes más comunes el "Tik Tok", es una de las más utilizadas, son presentaciones de videos, pero es muy común, el Facebook el Tinder son apetecidos para los menores de edad; son como redes de chat.

2.- ¿Qué tan complejo es el proceso de investigación para dar con los autores de este tipo de delitos; y por qué? Es un poco complicado, ya que la tecnología actual es de mensajes insertados, antes podíamos tener alcance con la cabecera de los mensajes o publicaciones, en Facebook, Twitter incluso de Instagram, y podíamos tratar de ubicar el IP, pero con los mensajes insertados ahí se desprende únicamente el mensaje, y se va con todo e IP; eso se lo hace para que

la red sea más veloz, y para que las redes tengan más acogida, ante esa instancia es más complicado tratar de ubicar el IP, que es el número que se le da a un usuario de internet; y la operadora puede ubicar en donde está instalado, podemos oficiar a la empresa proveedora de las redes sociales, hay que hacer un oficio con Fiscalía pero allá en EEUU ellos arman un expediente y mandan al Juez quien tendrá que despachar, y despachan a los 6 meses un año; entonces pasa mucho tiempo para que en Ecuador ya la instrucción se cierra o se cansa la víctima.

3.- ¿De su experiencia como perito que interviene en audiencias, cuantos casos de ciberdelitos, en contra de niños, niñas o adolescentes, han merecido sentencia condenatoria? Hemos llegado con casos a juicio, pero hay casos que no se puede determinar al responsable, cuando hablamos de cuentas no hablamos de personas sino de perfiles y atrás del perfil puede estar otra persona no necesariamente la del perfil, se han dado casos en forma femenina o masculina al otro lado no sabemos quién maneja la cuenta. En cuanto a niños niñas o adolescentes por pornografía no he tenido la oportunidad de ir a juicio.

De las entrevistas a los peritos, expertos en el tema de cibercriminalidad, se colige claramente, que los niños, niñas y adolescentes, son víctimas comunes de la ciberdelincuencia, dada la amplia gama de redes sociales, de entre ellas, algunas como Tik Tok que les resulta más llamativa, ello debido a su ingenuidad propia del desarrollo psicológico, lo que los hace más propensos y vulnerables; también ha quedado claro, que la actividad probatoria resulta compleja al momento de investigar el ciberdelito, y también se concluye que la judicialización de estos casos, resulta siendo escasa, dada la tormentosa tarea para endilgar responsabilidad a una persona, así como la renuncia de las víctimas, en tanto que el trámite se vuelve tedioso, lo que inclusive es configurativo de revictimización.

Propuesta

El Estado tiene como obligación prevenir la comisión de delitos; así lo consagra el Art 393 de la Constitución del Ecuador (2008) cuando determina, que el aparato estatal debe garantizar la seguridad, y con ello la integridad del individuo, mediante políticas y acciones integrales, con la finalidad de coadyuvar y asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir todas las formas de violencia y discriminación, así como la comisión de delitos;

es decir, constitucionalmente, el Estado, tiene la obligación positiva de prevenir, la comisión de cualquier delito que afecte bienes jurídicos.

El Art. 66 numeral 3 de la CRE consagra: El derecho a la integridad personal, que incluye: "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)

Existen varias formas de prevenir el cometimiento de ciberdelitos; empero, la principal es la educación; así, en escuelas, colegios y universidades, deben ser constantes las campañas que adviertan en lenguaje acorde a la edad y desarrollo de los menores de edad, los riesgos que implica el uso de redes sociales, en forma abierta y sin restricción; pero a más de ello, también campañas masivas para la gente adulta, a efectos de que puedan tomar las precauciones en casa con sus hijos o familiares, por una parte, pero por otra, que conozcan como actuar en caso de enterarse del cometimiento de estos ciberdelitos.

Si bien es cierto en nuestro país, se expidió la "*Ley Orgánica Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos*"; la misma recién entra en vigencia el 30 de agosto del 2021, es decir a pocos meses de la elaboración de este trabajo; así, nos damos cuenta de la lentitud estatal en cuanto a tipificar y sancionar las conductas ciberdelincuencia les, que, como se ha expresado en líneas precedentes, tiene un avance exponencial cada día.

Otro nudo crítico, en cuando al actuar estatal, es la falta de suscripción y ratificación del Convenio de Budapest, el cual se erige como el más importante instrumento internacional Hard Law, en la lucha contra la ciberdelincuencia, a nivel internacional, pues recoge directrices claras para los Estados en cuanto a temas álgidos como el de competencia territorial en el juzgamiento de estos delitos, así tambien, contiene definiciones importantes en el campo de la ciberdelincuencia, contiene medidas que se deben adoptar a nivel interno de los países suscriptores en cuanto al derecho sustantivo, pero también en cuanto al derecho adjetivo o

procesal, la jurisdicción, y la cooperación internacional; es decir, elementos trascendentes, para fortalecer la prevención, investigación, sanción y reparación por el cometimiento de estos ilícitos informáticos; empero de todo lo expuesto, el Ecuador no lo lo ha suscrito, como si lo han hecho Argentina, Perú, Colombia, Costa Rica y México; así, la Asociación Ecuatoriana de Ciberseguridad (AECI); se encuentra impulsando que el Ecuador sea parte de este convenio como una herramienta que permita a los gobiernos prestarse colaboración mutua en el campo, preventivo, jurídico y probatorio. (Budapest, 2021)

Así, siendo uno de los deberes primordiales del Estado, el precautelar el respeto de los derechos; con esta clase de delitos y su incipiente y todavía no suficiente prevención y legislación, se estaría limitando el hacer efectivo una amplia gama de los mismos entre ellos precisamente, el de la vida, integridad, indemnidad, la privacidad, intimidad, etc.; y, teniendo en cuenta el contexto y la edad de las actuales víctimas, se estarían lesionando el derecho al desarrollo e integridad personal tanto física psíquica, moral y sexual, así como el derecho a una vida libre de violencia para los niños, niñas y adolescentes.

Conclusiones

Cierto es que los nuevos avances de la ciencia y la tecnología van configurando una nueva era para la humanidad (Erraez, 2009, pág. 15). El uso temprano de las nuevas tecnologías informáticas y pautas educativas en torno a su manejo, depende en gran medida del hogar y vigilancia de los progenitores, pues son los menores quienes carecen de consciencia en torno a la importancia de la privacidad, sin llegar a dimensionar la repercusión respecto de la ausencia de límites en el mundo de las tecnologías; no obstante, es de trascendental importancia, advertir la desidiosa intervención del Estado, pues es evidente la ausencia de componentes o mecanismos de protección y prevención de cibercriminalidad a menores de edad.

Ha sido aprobada, recientemente la “Ley Orgánica Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos.”; lo que da cuenta del inoportuno y lento actuar estatal, ante el dinamismo acelerado del ciberespacio, como lugar en el que se cometen a diario delitos en contra de este grupo vulnerable.

La cibercriminalidad afecta a bienes jurídicos, que se encuentran constitucionalmente consagrados como son; la vida, la integridad personal, que incluye, a integridad, física psíquica, moral y sexual, una vida libre de violencia, en el ámbito público o privado y prohibición de tortura. El derecho a tomar decisiones libres, informadas, voluntarias y responsables sobre su sexualidad, su vida y orientación sexual. El Derecho al honor, buen nombre y la imagen. Derecho a la protección de datos de carácter personal; derecho a la intimidad personal y familiar; inviolabilidad de secreto y correspondencia, física y virtual.

Con la presente investigación se ha puesto en evidencia, tres inconvenientes en la lucha contra el cibercrimen en el Ecuador, estos son la revictimización, la dificultad probatoria y la desidia estatal; proponiendo en cuanto a la revictimización una adecuación normativa al Código Orgánico Integral penal, como garantía normativa consagrada en el Art, 84 de la Carta Constitucional; en cuanto a la dificultad probatoria, mediante expertos, hacer notar lo complejo que resulta en el dinamismo judicial la investigación y sanción de este tipo de delitos; y, en cuanto a la desidia estatal, colegir, que el Estado actúa en forma no oportuna en cuanto a legislar y prevenir este tipo de delitos, a más de ello, su falta de compromiso internacional al no ser suscriptor del Convenio de Budapest, como principal Instrumento Internacional de lucha contra la ciberdelincuencia.

Referencias

1. Aboso, G. E., & Zapata, M. F. (2006). Cibercriminalidad y Derecho Penal. Montevideo: IBdF.
2. Alajia, A., de la Luca, J., & Slokar, A. (2014). Derecho Penal. Delitos Informáticos. Buenos Aires: Infojus.
3. Ana, S., 1995 kierkegaard, S., & 2008. (2000). Granja, Pedro. Ecuador: Compilador.
4. Asamblea Nacional. (20 de octubre de 2008). Constitución de la República del Ecuador. Ecuador. Recuperado el 21 de septiembre de 2020, de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

5. Bokensford, E.-W. (2010). Sobre la situación de la dogmática de los derechos fundamentales tras 40 años de la ley Fundamental. En J. Z. Egas, Derecho Constitucional, Neoconstitucionalismo y Arguentación Jurídica (pág. 55). Guayaquil: Edilex.
6. Budapest, L. A. (6 de julio de 2021). it ahora.com. Obtenido de it ahora.com: https://itahora.com/2021/07/06/la aeci-impulsa-participacion-de-ecuador-en-el-convenio-de-budapest/
7. Carolina, V. (2020). Propuesta sexual telemática a menores. Ecuador: Compilador.
8. Carpio, D. S. (2013). El Delito Informático y la prueba Pericial Informática. Quito: jurídica del Ecuador.
9. Carpio, D. S. (2013). El Delito Informático y la Prueba Pericial Informática. Quito: Jurídica del Ecuador.
10. Davara Rodríguez, M. A. (1990). Análisis de la Ley de Fraude Informático. México DF: Revista de Derecho de la UNAM.
11. Dupuy, D., & Kiefer, M. (2018). CIBERCRIMEN. Montevideo, Uruguay: Ibdef.
12. Erraez, H. D. (2009). Los Términos de la Sociedad de la información y la Prospectiva. Cuenca,: Gráficas Hernández.
13. Granja, P. (2020). Internet y Pederastas . Ecuador: Compilador.
14. GuillesPie. (2020). Internet y Pederastas Granja. Compilador.
15. Iberoamericana, X. C. (6 de marzo de 2008). REGLAS DE BRASILIA SOBRE ACCESO A LA JUSTICIA DE LAS PERSONAS EN CONDICIÓN DE VULNERABILIDAD. REGLAS DE BRASILIA SOBRE ACCESO A LA JUSTICIA DE LAS PERSONAS EN CONDICIÓN DE VULNERABILIDAD. Brasilia, Brasilia, Brasil.
16. Martín, R. M. (2003). Delincuencia Informática y Derecho Penal. Vallodolid. España: Hispamer.
17. Martín, R. M. (2003). Delincuencia Informática y Derecho Penal. Vallodolid. España: Hispamer.
18. Navarro, M. d. (2015). Bullying, ciberbullyin y sexting ¿cómo actuar ante una situación de acoso? España: Ediciones Pirámide.
19. Palacios, D. L. (2009). Atención integral a las víctimas de violaciones a los derechos humanos. Algunos apuntes desde la victimología. REVISTA IIDH, 221.

20. Palacios, D. L. (2009). Atención integral a las víctimas de violaciones a los derechos humanos. Algunos apuntes desde la victimología. REVISTA IIDH, 217.
21. Pedro, G. (2020). Internet y Pederastas. Ecuador: Compilador.
22. Pozo, A. D. (7 de octubre de 2021). cibercrimen en niños, niñas y adolescentes. (D. C. Verdugo, Entrevistador)
23. Roxin, C. (1997). Derecho Penal Parte General Tomo I. Bonn Alemania: Civitas.
24. Solar, L. C. (1978). Explicaciones del Derecho Civil Chileno y Comparado. De las Obligaciones. Santiago de Chile: Editorial Jurídica de Chile.
25. Torres, G. C. (1993). Diccionario Jurídico Elemental. Buenos Aires: Heliasta S.R.L.
26. Villacampa. (2020). Internet y Pederastas Pedro Granja. Compilador.
27. Villacampa. (2020). Internet y Pederastas Pedro Granja. Compilador.
28. Zaruma, J. C. (27 de octubre de 2021). Ciberdelitos en niños niñas y adolescentes. (D. C. Verdugo, Entrevistador)