Universidad de Las Américas

Maestría en Derecho Penal con Mención en Criminalidad Compleja

-Ensayo Académico-

El delito de pornografía infantil en el Ecuador dificultades investigativas

Christian Alex Fierro Fierro

Quito, julio de 2024

RESUMEN

El aumento del delito de pornografía infantil en Ecuador y su relación con el ciberespacio plantean importantes problemas para la protección de los derechos de los niños, niñas y adolescentes (NNA), y la persecución de los perpetradores. Aunque se han intentado tipificar y resolver este delito desde 2005, su complejidad y el avance tecnológico siguen obstaculizando su investigación y enjuiciamiento. El propósito de esta investigación es examinar cómo las limitaciones tecnológicas, como el uso común de direcciones IP IPV4, afectan la capacidad de las autoridades de Quito para identificar y procesar a los responsables de este delito. La cuestión principal de este estudio es: ¿Cuál es el impacto de las direcciones IPV4 en la investigación del delito de pornografía infantil en Quito? Para responder a esta pregunta, se plantean objetivos específicos, como determinar cómo el ciberespacio está relacionado con el delito de pornografía infantil y demostrar cómo las direcciones IPV4 afectan la investigación del delito. La presente investigación utiliza la revisión bibliográfica y la entrevista a expertos con experiencia en el ámbito de la pornografía infantil como técnicas de recopilación de información. Los datos se analizan cualitativamente mediante técnicas de análisis de contenido aplicando el método analítico sintético y deductivo para procesar y examinar los resultados obtenidos. Posteriormente se realiza una triangulación de los datos, poniendo en comparación la información recopilada a través de la entrevista y la revisión bibliográfica.

Palabras claves: Ciberespacio, delito, pornografía infantil, direcciones IP, NCMEC Centro Nacional para Niños Desaparecidos y Explotados.

ABSTRACT

The increase in the crime of child pornography in Ecuador and its relationship with cyberspace pose significant challenges for the protection of children's rights and the prosecution of perpetrators. Although this crime has been criminalized and attempts have been made to resolve it since 2005, its complexity and technological advancement continue to hinder its investigation and prosecution. The purpose of this research is to examine how technological limitations, such as the common use of IPv4 addresses, affect the ability of Quito authorities to identify and prosecute those responsible for this crime. The main question of this study is: What is the impact of IPv4 addresses on the investigation of child pornography crime in Quito? To answer this question, specific objectives are proposed, such as determining how cyberspace is related to the crime of child pornography and demonstrating how IPv4 addresses affect the investigation of the crime. This research uses literature review and interviews with experts experienced in the field of child pornography as information gathering techniques. The data is analyzed qualitatively using content analysis techniques applying the synthetic and deductive analytical method to process and examine the results obtained. Subsequently, a triangulation of the data is carried out, comparing the information collected through the interview and the literature review.

Keywords: Cyberspace, crime, child pornography, IP addresses, NCMEC National Center for Missing and Exploited Children.

Contenido

Índice de Figuras

INTRODUCCIÓN

El delito de pornografía infantil representa una de las más graves violaciones a los derechos humanos y la dignidad de los NNA en el mundo contemporáneo. En Ecuador, este problema ha cobrado una relevancia particular debido a la creciente digitalización de la sociedad y el aumento del acceso a internet, especialmente entre los más jóvenes. Este fenómeno, que se encuentra en la intersección de la tecnología, la criminalidad y la protección de los NNA plantea desafíos complejos y multifacéticos para las autoridades, los legisladores y la sociedad en general.

La presente investigación se propone examinar en profundidad la situación actual del delito de pornografía infantil en Ecuador, con un enfoque particular en las dificultades investigativas que enfrentan las autoridades. Este estudio abarca desde la evolución histórica y legal del delito en el país hasta los más recientes desafíos tecnológicos y operativos que complican su persecución y prevención.

Un aspecto central de este análisis es el impacto de las limitaciones tecnológicas, específicamente el uso generalizado de direcciones IP IPv4, en la capacidad de las autoridades para identificar y procesar a los responsables de estos crímenes. Esta problemática se examina en el contexto más amplio de la ciberseguridad y la protección de los derechos de los NNA.

Además, se explora la crucial importancia de la cooperación internacional en la lucha contra este delito transnacional, evaluando la adhesión de Ecuador a instrumentos como el Convenio de Budapest y su implementación práctica. Se analiza también el papel de organizaciones internacionales como el National Center for Missing & Exploited Children (NCMEC) Centro Nacional para Niños Desaparecidos y Explotados, en la detección y reporte de casos.

Se examina la diferencia entre los casos de "sexting" entre adolescentes y la explotación sexual infantil en el marco del crimen organizado, subrayando la necesidad de respuestas diferenciadas y proporcionales.

A lo largo de la investigación, se integran perspectivas de diversos actores, incluyendo fiscales especializados, investigadores policiales nacionales e internacionales, expertos en tecnología y organizaciones de protección infantil. Este enfoque multidisciplinario permite una comprensión más completa y matizada del problema.

El objetivo final de este trabajo es no solo proporcionar un análisis exhaustivo de la situación actual, sino también ofrecer recomendaciones concretas y factibles para fortalecer la lucha contra la pornografía infantil en Ecuador. Estas propuestas abarcan desde mejoras en las capacidades tecnológicas de las instituciones, marco legal y hasta estrategias de prevención y educación.

En un mundo donde la tecnología evoluciona rápidamente y los criminales adaptan constantemente sus métodos, esta investigación busca contribuir a la protección efectiva de los NNA en el entorno digital, promoviendo un enfoque integral que equilibre la persecución del delito con la prevención y el apoyo a las víctimas. La urgencia de abordar este problema de manera efectiva no puede ser subestimada, ya que cada caso de pornografía infantil representa una violación inaceptable de los derechos y la integridad de los más vulnerables de nuestra sociedad.

La presente investigación adopta un enfoque cualitativo como método analítico, sintético y deductivo. Como técnicas de recolección de información, se ha realizado una revisión bibliográfica exhaustiva y se han llevado a cabo entrevistas a expertos e investigadores con amplia experiencia en el ámbito de la pornografía infantil (Creswell, 2014).

La revisión bibliográfica ha permitido examinar en profundidad la evolución histórica y legal del delito de pornografía infantil en Ecuador, así como los desafíos tecnológicos y operativos que enfrentan las autoridades en su persecución y prevención (UNICEF, 2020). Se han consultado fuentes académicas, informes gubernamentales, documentos internacionales y publicaciones especializadas para obtener una comprensión integral del problema. Adicionalmente, las entrevistas semiestructuradas han brindado perspectivas valiosas desde diferentes ámbitos, permitiendo una comprensión más matizada y multidisciplinaria del fenómeno de la pornografía infantil en el país.

El enfoque cualitativo, que permite captar el conocimiento, el significado y las interpretaciones compartidas por los individuos sobre la realidad social estudiada (Bonilla, 1997, p. 18), ha sido crucial para detallar los desafíos y complejidades de este delito y para identificar soluciones y recomendaciones adaptadas al contexto ecuatoriano. El método analítico, sintético y deductivo, que genera un análisis mediante la síntesis de propiedades y características (Rodríguez, 2017, p. 186), ha facilitado la integración de la información recopilada y la formulación de conclusiones y propuestas concretas para fortalecer la lucha contra la pornografía infantil en Ecuador.

Problemática jurídica planteada y metodología:

La problemática jurídica central de esta investigación es el delito de pornografía infantil en Ecuador y las dificultades que enfrentan las autoridades para investigarlo efectivamente, sobre todo en el entorno digital.

Específicamente, el estudio aborda:

1. La complejidad de investigar este delito en el ciberespacio debido a limitaciones tecnológicas, como el uso generalizado de direcciones IP versión 4 (IPv4) que dificultan la identificación precisa de usuarios.

2. Los desafíos legales y procedimentales, incluyendo la falta de adhesión de Ecuador al Convenio de Budapest sobre Ciberdelincuencia, que limita la cooperación internacional.

3. La escasez de recursos humanos y tecnológicos especializados en las instituciones encargadas de investigar estos delitos.

4. La necesidad de actualizar y adaptar el marco legal para abordar las nuevas formas de explotación sexual infantil en línea.

5. La tensión entre la protección de la privacidad en línea y la necesidad de investigar eficazmente estos delitos.

Metodología:

El estudio emplea un enfoque cualitativo con métodos analíticos, sintéticos y deductivos. Las principales técnicas de recolección de datos son:

1. Revisión bibliográfica exhaustiva de fuentes académicas, informes gubernamentales, documentos internacionales y publicaciones especializadas.

2. Entrevistas semiestructuradas a expertos de diversos ámbitos:

- Autoridades policiales (Ing. Teniente Coronel Gonzalo García)
- Fiscales especializados (Dra. Silvana Paola Solís Cabrera)
- Investigadores criminales de la Oficina de Investigaciones del Departamento de Seguridad Nacional de Los Estados Unidos de América (Miguel Salazar, Ricardo Ramírez, Israel Loor)
-Especialistas en ciberseguridad (Ing. Jorge C. Guerrón Eras, Ing. José María Gómez de la Torre)

3. Análisis de casos y estadísticas proporcionadas por organizaciones como el National Center for Missing & Exploited Children (NCMEC).

4. Estudio comparativo de modelos internacionales, como la plataforma TeProtejo de Colombia.

El análisis de datos se realiza mediante técnicas de análisis de contenido, aplicando el método analítico sintético y deductivo. Se emplea la triangulación de datos para comparar y contrastar la información obtenida de diferentes fuentes, buscando patrones, tendencias y discrepancias.

Esta metodología permite una comprensión profunda y multidimensional del problema, integrando perspectivas tecnológicas, operativas y legales. El enfoque cualitativo facilita la exploración de las complejidades y matices del tema, mientras que la diversidad de fuentes y expertos consultados enriquece el análisis y las recomendaciones resultantes.

PRIMERO

EL DELITO DE PORNOGRAFÍA INFANTIL

1.1 La presente investigación aborda el grave problema del delito de pornografía infantil, analizando sus causas, consecuencias y las estrategias necesarias para su prevención, investigación y sanción.

1.2 Concepto de Pornografía Infantil

Según la ONU (2000), la pornografía infantil se define como cualquier representación que muestra a menores involucrados en actividades sexuales explícitas o la exhibición de sus genitales con propósitos predominantemente sexuales. Este enfoque no solo abarca imágenes y videos, sino también escritos y cualquier otro medio que pueda transmitir tales representaciones.

El Convenio sobre la Ciberdelincuencia Budapest (2001) amplía esta definición, incluyendo cualquier material visual que represente a menores participando en conductas sexualmente explícitas, ya sea en actuaciones explícitas o simuladas, o incluso imágenes realistas que sugieran tal comportamiento.

En tal sentido, la terminología utilizada para describir la explotación sexual de menores ha sido objeto de intenso debate en los últimos años. El término "pornografía infantil", ampliamente utilizado en el pasado, ha sido cada vez más cuestionado por investigadores, profesionales y defensores de los derechos de los niños.

Una de las principales críticas al término "pornografía infantil" es que puede minimizar la gravedad del delito. Como argumenta Gillespie (2018), "el uso del término 'pornografía' sugiere erróneamente que este material es una forma de entretenimiento para adultos, en lugar de evidencia de un grave abuso contra un niño" (p. 289). Esta percepción errónea puede tener consecuencias significativas en cómo la sociedad y el sistema legal abordan estos crímenes.

En respuesta a estas preocupaciones, muchos expertos y organizaciones han abogado por el uso del término "material de abuso sexual infantil" (MASI) como una alternativa más precisa y éticamente apropiada. Este término enfatiza la naturaleza abusiva del contenido y centra la atención en la victimización de los NNA. Como señala INTERPOL (2019), "el término MASI refleja con mayor precisión la verdadera naturaleza de este contenido, que es la documentación de un delito grave contra un niño".

Sin embargo, el cambio terminológico no está exento de desafíos. Uno de los principales obstáculos es la prevalencia del término "pornografía infantil" en la legislación existente. Como observa Dodge (2018), "la transición a una nueva terminología puede crear inconsistencias legales y dificultar la aplicación de la ley si no se implementa de manera uniforme" (p. 712).

Además, el término MASI también ha sido objeto de críticas. Algunos argumentan que no abarca completamente el espectro de material explotador que involucra a niños. Por ejemplo, el "material de explotación sexual infantil" (MESI) se ha propuesto como un término más amplio que incluiría imágenes que, aunque no muestran abuso sexual directo, aún explotan sexualmente a los niños (Canadian Centre for Child Protection, 2019).

Otro aspecto crucial del debate terminológico es la distinción entre "niño" y "menor". Mientras que "niño" generalmente se refiere a individuos prepúberes, "menor" puede incluir a adolescentes hasta la edad de 18 años. Esta distinción es importante no solo desde una perspectiva legal, sino también para comprender y abordar las diferentes formas de explotación que pueden ocurrir en diferentes etapas del desarrollo (Quayle & Cooper, 2015).

La evolución de la tecnología también ha planteado nuevos desafíos terminológicos. Con el surgimiento de material generado por IA y deepfakes, surge la pregunta de cómo clasificar y abordar el material que parece mostrar abuso sexual infantil pero que no involucra a un niño real. Algunos han propuesto el término "material de abuso sexual infantil simulado" para estos casos, aunque su estatus legal y ético sigue siendo objeto de debate (Hessick, 2017).

Según la Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores de edad y la pornografía infantil, el acceso a la pornografía infantil, ya sea real o simulada, debe tipificarse como infracción penal si la persona tiene la intención de acceder a ese tipo de contenido y sabe que es posible encontrarlo en el sitio web. La directiva define la "pornografía infantil" como: “todo material que represente de manera visual a un menor participando en una conducta sexualmente explícita, real o simulada” (Directiva 2011/92/UE, Art. 2).

El lenguaje utilizado para describir a las víctimas también ha sido objeto de escrutinio. Términos como "víctima de pornografía infantil" han sido criticados por potencialmente etiquetar y estigmatizar a los niños. En su lugar, frases como "niño que

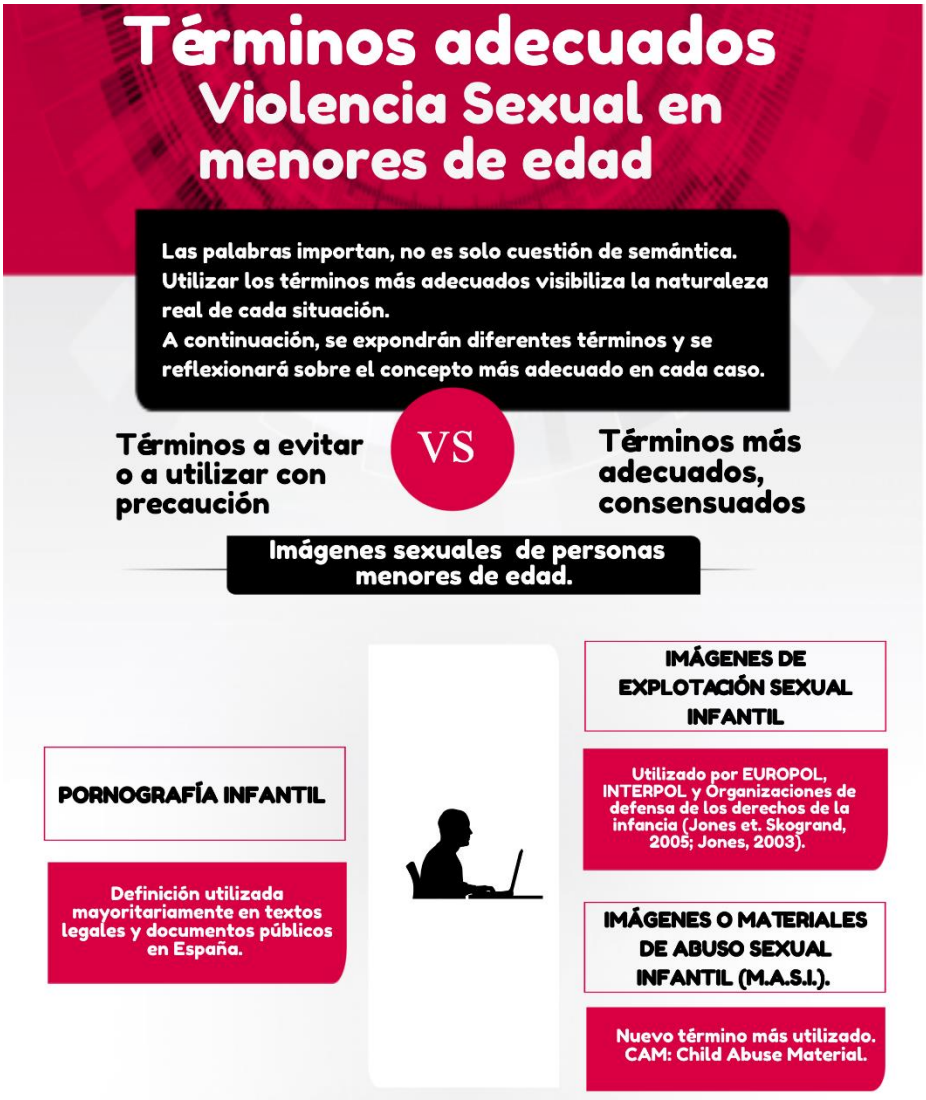
ha sido abusado sexualmente" o "sobreviviente de abuso sexual infantil" se consideran más respetuosas y centradas en el niño (ECPAT International, 2016). Los términos propuestos, si bien intentan ser más respetuosos, aún pueden ser estigmatizantes. Es crucial utilizar un lenguaje cuidadoso y sensato cuando se habla de niños que han experimentado abuso sexual. En lugar de etiquetar a los niños, se puede hacer énfasis en su proceso de recuperación y sanación, como "niños en proceso de recuperación" o "niños que están recibiendo apoyo".

El objetivo es utilizar un lenguaje que respete la privacidad y la integridad de los NNA, sin hacer énfasis en su condición de víctimas. Frases como "niños que han sido tratados con crueldad" o "niños que han experimentado situaciones difíciles" pueden ser más apropiadas. La idea es evitar términos que puedan estigmatizar o revictimizar a los NNA, y en su lugar, enfocar el lenguaje en su humanidad, su proceso de sanación y su dignidad como personas.

Es importante reconocer que la terminología no es solo una cuestión semántica, sino que tiene implicaciones reales en cómo se percibe, investiga y procesa el abuso sexual infantil. Como argumenta Taylor (2018), "el lenguaje que usamos moldea nuestras percepciones y, por extensión, nuestras respuestas a estos crímenes. Una terminología más precisa y ética puede conducir a mejores resultados para las víctimas y una aplicación más efectiva de la ley" (p. 423).

Sin embargo, también es crucial reconocer que el cambio terminológico por sí solo no es suficiente para abordar el problema subyacente del abuso sexual infantil. Como advierte Salter (2017), "existe el riesgo de que el debate sobre la terminología desvíe la atención y los recursos de las intervenciones prácticas necesarias para prevenir el abuso y apoyar a las víctimas" (p. 35).

Figura 1 ***Términos adecuados***



Nota. Adaptado de Términos adecuados Violencia sexual [INFOGRAFÍA], por Asociación rea, s.f.

1.3 Evolución histórica del delito de pornografía infantil en el Ecuador

En Ecuador, es fundamental examinar cómo han influido las modificaciones legales, los avances tecnológicos y la conciencia social en la protección de los derechos de los NNA. En términos normativos internacionales, la Convención sobre los Derechos del Niño y sus protocolos han sido piedras angulares. Estos instrumentos internacionales obligan a los Estados Parte, incluido Ecuador, a adoptar medidas para prevenir y penalizar la explotación infantil en contextos pornográficos (CDN, 1990). A nivel nacional, el

Código de la Niñez y Adolescencia, promulgado en 2003, establece prohibiciones explícitas contra la participación de menores en producciones pornográficas y espectáculos inapropiados para su edad (Código de la Niñez y Adolescencia, 2003).

La base legal se fortaleció con reformas al Código Penal en 2005, que impusieron sanciones significativas para quienes produzcan, publiquen, distribuyan o faciliten acceso a material pornográfico que involucre a NNA. Estas reformas reflejan el compromiso de Ecuador con las normativas internacionales y la protección de la infancia frente a la explotación sexual (Reformas al Código Penal, 2005). Este marco legal integral no solo tipificaba el delito de pornografía infantil, sino que también abarcaba toda la cadena de producción y distribución del material ilícito. Sin embargo, la efectividad de estas leyes se ve desafiada por los avances tecnológicos, que facilitan la difusión rápida y global de contenido perjudicial para los NNA.

Estas reformas impusieron sanciones severas para quienes produzcan, publiquen, distribuyan o faciliten el acceso a material pornográfico que involucre a NNA. El artículo sin número añadido al capítulo de delitos de explotación sexual en 2005 establecía penas de reclusión de 6 a 9 años por la producción, publicación o comercialización de imágenes pornográficas con participación de menores de 14 a 18 años. Además, la distribución de material pornográfico con imágenes de menores de 12 a 18 años también se castigaba con la misma pena.

En los casos donde la víctima sea menor de 12 años, discapacitada o con enfermedad grave, la pena se elevaba a reclusión mayor extraordinaria de 12 a 16 años. Incluso, la reincidencia se sancionaba con reclusión mayor especial de 25 años. Además, se establecían penas de 16 a 25 años para familiares, autoridades y profesionales que hayan abusado de la víctima.

Estas reformas reflejan el compromiso de Ecuador con las normativas internacionales y la protección de los NNA frente a la explotación sexual. Sin embargo, la efectividad de estas leyes se ve desafiada por los avances tecnológicos, que facilitan la rápida y global difusión de contenido perjudicial para los NNA.

Es decir, el marco legal ecuatoriano ha evolucionado para tipificar y sancionar severamente el delito de pornografía infantil, abarcando toda la cadena de producción y distribución del material ilícito. No obstante, los desafíos tecnológicos plantean la necesidad de una constante adaptación y mejora de las estrategias de prevención y persecución de este delito (Reformas al Código Penal, 2005).

Constitución de la República del Ecuador

La Constitución de la República del Ecuador de 2008 enfatiza el deber del Estado, la sociedad y la familia de promover el desarrollo integral de los NNA, asegurando el pleno ejercicio de sus derechos fundamentales. Se establece el principio de interés superior de los NNA y que sus derechos deben prevalecer sobre los de cualquier otra consideración. Este desarrollo integral implica la creación de un entorno seguro y afectivo que satisfaga sus necesidades sociales, emocionales y culturales, con el respaldo de políticas intersectoriales a nivel nacional y local.

Asimismo, la Constitución especifica la obligación de establecer procedimientos legales rápidos y específicos para enjuiciar y sancionar delitos que afecten a grupos vulnerables, incluyendo niñas, niños y adolescentes. Esto se refleja en la designación de fiscales y defensores especializados para abordar estos casos, conforme al artículo 81 de la ley suprema.

Es crucial profundizar en cómo estas disposiciones constitucionales se traducen en la práctica judicial y administrativa. Esto implica evaluar la efectividad de los procedimientos legales especiales en la protección de los derechos de los NNA frente a delitos como la violencia sexual y otros crímenes que los afecten. Además, es importante analizar los desafíos y las barreras que enfrentan las instituciones encargadas de aplicar estas leyes, así como las percepciones y participación de la sociedad civil en el cumplimiento de estos derechos.

Además, se debe considerar el contexto socioeconómico y cultural del país, ya que estos factores influyen en la efectividad de las políticas y en la protección real de los derechos de los NNA. Además, se puede explorar comparativamente cómo otros países enfrentan estos desafíos y qué lecciones pueden aplicarse en el contexto ecuatoriano.

Código Orgánico Integral Penal

El Código Orgánico Integral Penal (COIP), promulgado en 2014, introdujo disposiciones significativas en relación con la pornografía infantil. El artículo 103 del COIP tipifica y sanciona severamente la producción de material visual, audiovisual, informático o electrónico que represente a NNA en actitudes sexualmente explícitas. Este artículo no solo prohíbe la producción de tales contenidos, sino que también considera circunstancias agravantes, como la discapacidad de la víctima o la relación cercana del infractor con ella.

Por otro lado, el artículo 104 del COIP aborda la comercialización de pornografía infantil, estableciendo penas para aquellos que publiciten, compren, posean, transmitan, importen, exporten o vendan material pornográfico que involucre a NNA. Esta disposición amplía la responsabilidad penal a todas las etapas de la cadena de distribución y posesión de este tipo de material.

Es crucial destacar que el COIP reestructuró estas disposiciones, separándolas del capítulo de delitos sexuales para integrarlas en un marco más amplio de graves violaciones a los derechos humanos y delitos contra el derecho internacional humanitario. Estableciendo penas que van desde los 13 a 16, 16 a 19 y 22 a 26 años de penas privativas de libertad. Esta reubicación refleja un enfoque más integral hacia la protección de los derechos de los NNA y una respuesta más efectiva frente a las complejidades tecnológicas y legales actuales.

Desde una perspectiva crítica, es fundamental evaluar cómo estas disposiciones han sido implementadas en la práctica judicial ecuatoriana. La eficacia en la investigación, persecución y sanción de los delitos de pornografía infantil es crucial para garantizar la protección efectiva de los derechos de los NNA. Además, es necesario considerar las dificultades inherentes a la aplicación de estas leyes en un contexto internacional, donde la circulación transfronteriza de contenido ilícito presenta desafíos significativos para las autoridades.

Además de la evaluación legal y operativa, es pertinente discutir la terminología utilizada en estas disposiciones legales. La definición de "pornografía infantil" en el COIP debe analizarse en el contexto de las normativas internacionales y las prácticas judiciales locales para determinar su adecuación y efectividad en la protección de los derechos de los NNA.

1.4 Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía

El Protocolo facultativo, adoptado por la Asamblea General de las Naciones Unidas en 2000, representa un hito crucial en la lucha contra la explotación sexual infantil. Sin embargo, su implementación y efectividad han sido objeto de debate y crítica.

Uno de los aspectos más controvertidos del Protocolo es su enfoque en la criminalización. Aunque establece claramente la necesidad de tipificar como delito la venta de niños, la prostitución infantil y la pornografía infantil, algunos críticos

argumentan que este enfoque puede, paradójicamente, poner en riesgo a los niños que pretende proteger. Como señala Gillespie (2012), "la criminalización puede llevar a la marginación y estigmatización de las víctimas, dificultando su acceso a servicios de apoyo y rehabilitación" (p. 87).

Otro punto de discusión es la definición de "niño" en el Protocolo. Aunque se establece como toda persona menor de 18 años, esta definición uniforme no tiene en cuenta las variaciones culturales y legales en diferentes países respecto a la mayoría de edad. Esta discrepancia puede crear desafíos en la implementación y aplicación del Protocolo a nivel internacional (UNICEF, 2019).

El Protocolo también ha sido criticado por su enfoque limitado en la prevención. Si bien establece la necesidad de medidas preventivas, no proporciona directrices específicas sobre cómo implementarlas efectivamente. Como argumenta Svevo-Cianci et al. (2011), "el énfasis en la criminalización a menudo eclipsa la importancia crucial de la prevención y la educación en la lucha contra la explotación sexual infantil" (p. 1196).

La cuestión de la jurisdicción extraterritorial, aunque abordada en el Protocolo, sigue siendo un área de preocupación. En un mundo cada vez más globalizado y digitalizado, la explotación sexual infantil a menudo trasciende las fronteras nacionales. El Protocolo insta a los Estados a establecer jurisdicción extraterritorial, pero la implementación práctica de esta disposición ha demostrado ser compleja y, en muchos casos, ineficaz (Gallagher, 2010).

Además, el Protocolo ha sido criticado por no abordar adecuadamente las nuevas formas de explotación sexual infantil facilitadas por la tecnología. Aunque se menciona la "pornografía infantil", el rápido avance de las tecnologías digitales ha dado lugar a nuevas formas de abuso, como la transmisión en vivo de abuso sexual infantil, que no están explícitamente cubiertas por el Protocolo (Quayle & Cooper, 2015).

Por último, la cuestión de la rehabilitación y reintegración de las víctimas, aunque mencionada en el Protocolo, carece de directrices concretas y mecanismos de implementación. Como señala Rafferty (2013), "la falta de un enfoque integral en la recuperación y reintegración de las víctimas representa una grave omisión en la respuesta global a la explotación sexual infantil" (p. 568).

1.5. El delito de pornografía infantil en el marco de la Convención de Budapest

El Convenio de Budapest sobre Ciberdelincuencia representa un hito importante en los esfuerzos internacionales para combatir los delitos cibernéticos, incluyendo la pornografía infantil. Sin embargo, un análisis crítico revela tanto sus fortalezas como sus limitaciones en el contexto actual.

El Convenio, adoptado en 2001, proporciona un marco legal común para abordar los delitos informáticos a nivel internacional (Consejo de Europa, 2001). No obstante, el rápido avance tecnológico desde su implementación ha planteado nuevos desafíos que el Convenio no aborda completamente. Como señala Barrio (2020), la pornografía infantil sigue siendo "uno de los fenómenos criminales más preocupantes" (p. 113), lo que sugiere que el Convenio no ha logrado frenar eficazmente este problema.

La adhesión de Ecuador al Convenio, aunque es un paso positivo, plantea interrogantes sobre la capacidad del país para implementar efectivamente sus disposiciones. Las reformas al Código Orgánico Integral Penal en 2023 demuestran un esfuerzo por alinear la legislación nacional con los estándares internacionales (Asamblea Nacional del Ecuador, 2023). Sin embargo, estas reformas podrían no ser suficientes para abordar las complejidades tecnológicas y jurisdiccionales del cibercrimen transnacional.

El enfoque del Convenio en la criminalización y la cooperación internacional, aunque necesario, podría no abordar suficientemente las causas fundamentales de la explotación sexual infantil en línea. Un enfoque más integral que incluya medidas preventivas, educativas y de rehabilitación podría ser más efectivo a largo plazo. (Martins dos Santos, 2021)

Además, el Convenio no aborda adecuadamente las nuevas formas de explotación sexual infantil facilitadas por la tecnología, como la transmisión en vivo de abuso sexual. Esta brecha en la cobertura del Convenio podría dejar a las víctimas vulnerables a formas emergentes de explotación.

La participación de múltiples instituciones en el proceso de adhesión de Ecuador al Convenio es loable. Sin embargo, la efectividad de esta colaboración interinstitucional en la práctica aún está por verse, especialmente considerando los desafíos de coordinación que a menudo enfrentan las agencias gubernamentales en la implementación de políticas complejas. (Martins dos Santos, 2021)

1.6 Childfund en Beneficio de los NNA

ChildFund es una organización internacional sin fines de lucro dedicada a mejorar las condiciones de vida de NNA en situación de vulnerabilidad en más de 20 países. Una de las principales estrategias de ChildFund es la implementación de programas de concienciación dirigidos a NNA, padres y educadores. Estos programas tienen como objetivo informar sobre los riesgos en línea y promover prácticas de navegación segura. Un caso emblemático es Ecuador, donde ChildFund, en colaboración con FENPIDEC, ha jugado un papel crucial en la creación de una ordenanza para un internet seguro. Esta normativa regula los servicios de cibercafés y establece medidas para prevenir la violencia en Internet (ChildFund Ecuador, 2023). Sin embargo, la sostenibilidad de estos programas depende de la continuidad del financiamiento y la capacitación constante de los facilitadores.

La institución ChildFund en Beneficio de los NNA se menciona en relación con la investigación sobre el delito de pornografía infantil en Ecuador debido a su papel en la protección y recuperación de NNA afectados por este tipo de delitos, aspectos que tanto la Fiscalía General del Estado y la Policía Nacional lo pasan por alto ya que se enfocan en un papel meramente reactivo o investigativo.

El fortalecimiento de capacidades es otro pilar fundamental en la labor de ChildFund. La organización se dedica a la capacitación de maestros, trabajadores sociales y personal de salud, dotándolos de herramientas para identificar y responder a los riesgos en línea que enfrentan los menores (ChildFund International, 2022). No obstante, un desafío significativo es la variabilidad en los recursos y la infraestructura entre los países donde opera ChildFund, lo que puede afectar la calidad y el alcance de la capacitación. En el ámbito de la abogacía y las políticas públicas, ChildFund desempeña un rol esencial. La organización colabora con gobiernos y entidades para fomentar la creación e implementación de políticas y leyes que protejan a los NNA en el entorno digital.

En Ecuador, por ejemplo, ChildFund ha sido clave en el desarrollo de la política pública para una internet segura (Ministerio de Telecomunicaciones y de la Sociedad de la Información de Ecuador, 2024). A pesar de estos avances, la implementación efectiva de estas políticas requiere un compromiso continuo de los gobiernos y la capacidad de adaptación a los cambios tecnológicos.

1.7 Política Pública por una Internet Segura para Niños, Niñas y Adolescentes

La Política pública por una internet segura para niños, niñas y adolescentes de Ecuador representa un esfuerzo significativo para abordar los desafíos y oportunidades que presenta el entorno digital para los menores. Este documento, desarrollado en 2020, reconoce la creciente importancia de las tecnologías digitales en la vida de los NNA y busca establecer un marco integral para su protección y empoderamiento en línea.

La política se fundamenta en la premisa de que el acceso a internet y las tecnologías digitales puede ser una herramienta poderosa para el desarrollo y el ejercicio de los derechos de los NNA, pero también conlleva riesgos significativos. Como se señala en el documento, "Las tecnologías de la información y la comunicación son parte de la vida cotidiana de niños, niñas y adolescentes, como mecanismo de acceso y uso de internet; interacción social y construcción de identidad" (Consejo Nacional para la Igualdad Intergeneracional [CNII], 2020, p. 32).

Un aspecto crucial de esta política es su enfoque multidimensional. No se limita a abordar los riesgos y peligros en línea, sino que también busca promover el uso positivo y constructivo de las tecnologías digitales. El documento establece que el objetivo es "potenciar las oportunidades y habilidades que ofrecen las tecnologías digitales en su vida y su desarrollo, y así, promover el aprovechamiento de los usos y beneficios de las TIC en un marco de derechos (digitales), dignidad e integridad física, psicológica, emocional y sexual" (CNII, 2020, p. 34).

La política se estructura en cinco ejes principales:

- Medidas Legales
- Medidas Técnicas y Procedimentales
- Seguimiento y control a través de la articulación y coordinación institucional
- Fortalecimiento y consolidación de capacidades y habilidades
- Estrategia comunicacional

En el eje de Medidas Legales, la política busca fortalecer y reformar la legislación nacional para garantizar los derechos digitales de los NNA. Esto incluye propuestas para modificar el Código de la Niñez y Adolescencia y el Código Orgánico Integral Penal. Por ejemplo, se propone "incluir los derechos digitales, la ciudadanía digital, las capacidades informacionales, las medidas de protección y reparación, y la tipificación y sanciones frente a las transgresiones y delitos cometidos contra de niñas, niños y adolescentes en entornos virtuales" (CNII, 2020, p. 47).

El eje de Medidas Técnicas y Procedimentales se enfoca en promover un acceso seguro y constructivo a las TIC. Esto implica el desarrollo de lineamientos técnicos, regulaciones y códigos de conducta para proteger a los NNA de contenidos nocivos y delitos en línea. Una acción clave en este eje es "Desarrollar e implementar mecanismos, lineamientos y medidas técnicas para la regulación y control del acceso a contenidos nocivos, transgresiones y posibles delitos en los servicios del régimen general de telecomunicaciones (TIC)" (CNII, 2020, p. 49).

El tercer eje, centrado en el seguimiento y control, busca establecer estructuras organizacionales para la implementación y evaluación de la política. Esto incluye la creación de una mesa técnica interinstitucional y la promoción de la cooperación internacional en materia de ciberseguridad y protección infantil en línea.

El cuarto eje se enfoca en el fortalecimiento de capacidades, reconociendo la importancia de la educación y la alfabetización digital. La política propone "Fortalecer la agenda educativa digital para potenciar y mejorar la calidad educativa, la cobertura y la garantía de derechos de niñas, niños y adolescentes con la participación de los actores educativos" (CNII, 2020, p. 57).

Finalmente, el quinto eje se centra en la estrategia comunicacional, buscando promover una cultura de protección integral de los NNA en el entorno digital. Esto incluye campañas de concientización y la difusión de información sobre el uso seguro de internet.

Un aspecto destacable de esta política es su enfoque participativo. El documento enfatiza la importancia de involucrar a los propios NNA en el diseño, implementación y evaluación de las medidas de protección en línea. Esto se refleja en acciones como "Promover la participación de niñas, niños y adolescentes en la implementación, seguimiento y evaluación de la política pública uso seguro de internet" (CNII, 2020, p. 53).

La política también reconoce la importancia de la colaboración intersectorial e internacional. Se propone la coordinación entre diversas instituciones gubernamentales, así como la cooperación con organismos internacionales y el sector privado. Por ejemplo, se plantea "Gestionar la adhesión del Estado ecuatoriano al 'Convenio sobre la ciberdelincuencia' (Convenio de Budapest)" (CNII, 2020, p. 54).

Un aspecto crítico abordado en la política es la necesidad de equilibrar la protección con el empoderamiento digital de los NNA. Se reconoce que las tecnologías digitales ofrecen oportunidades significativas para el aprendizaje, la creatividad y la

participación social de los menores. Por lo tanto, las medidas de protección no deben restringir indebidamente estas oportunidades.

La política también aborda la importancia de la investigación continua sobre los riesgos y oportunidades en línea para los NNA. Se propone "Realizar una encuesta nacional - regional acerca del uso del Internet por parte de niños, niñas y adolescentes" (CNII, 2020, p. 55), lo que permitiría adaptar las políticas a medida que evoluciona el panorama digital.

1.8 Análisis de Políticas Sobre Protección Infantil en Línea para AMS

El "Análisis de Políticas Sobre Protección Infantil en Línea para AMS" emitido por la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (IFRC por sus siglas en inglés). Esta política tiene un nivel de vínculo obligatorio para todas las organizaciones miembro de la IFRC, ya que establece un marco común para garantizar la protección de los niños en todos los programas e iniciativas de la Federación Internacional. Es decir, es una política de carácter vinculante y de cumplimiento obligatorio para las sociedades nacionales de la Cruz Roja y Media Luna Roja que forman parte de la IFRC.

Ofrece una visión comparativa de las estrategias implementadas por varios países de América Latina para salvaguardar a los niños, niñas y adolescentes (NNA) en el entorno digital. Este estudio, que incluye a Colombia, Costa Rica, Ecuador, México, Paraguay y Perú, revela tanto avances significativos como desafíos persistentes en la región.

Un hallazgo crítico del análisis es la disparidad en el desarrollo de políticas específicas para la protección infantil en línea. Mientras que países como Colombia, Costa Rica, Ecuador y Paraguay han diseñado políticas públicas y programas con un enfoque específico en NNA, México y Perú carecen de una estrategia nacional dedicada a este tema (Unión Internacional de Telecomunicaciones [UIT], 2021). Esta disparidad sugiere una necesidad urgente de una mayor atención y recursos dedicados a la protección infantil en línea en algunos países de la región.

El estudio destaca iniciativas innovadoras como "En TIC Confío +" de Colombia, un programa que promueve el desarrollo de habilidades digitales para enfrentar los riesgos asociados al uso de internet y las TIC (UIT, 2021). Sin embargo, es crucial evaluar

críticamente la efectividad de estos programas en términos de su alcance e impacto real en la seguridad de los NNA en línea.

Un aspecto preocupante revelado por el análisis es la falta de una legislación específica para la protección de NNA en línea en la mayoría de los países estudiados. Como señala el informe, "ninguno de ellos tiene una ley especial para la protección de niñas, niños y adolescentes en línea, y la legislación existente está dirigida a la violencia en el ciberespacio, o bien, a delitos de índole sexual" (UIT, 2021, p. 28). Esta brecha legal podría dejar a los NNA vulnerables a nuevas formas de explotación y abuso en el entorno digital.

El estudio también revela una falta de datos consistentes y comparables sobre el uso de internet por parte de los NNA en la región. Por ejemplo, se menciona que "Gran parte de los estudios estadísticos, no dan cuenta de mediciones para grupos de edad menores de 15 años, lo cual deja cierto aire de incertidumbre frente al uso de las tecnologías digitales en niños, niñas y adolescentes" (UIT, 2021, p. 13). Esta falta de datos dificulta la formulación de políticas basadas en evidencia y la evaluación efectiva de las intervenciones existentes.

Un aspecto positivo es el reconocimiento de la importancia de la colaboración internacional en la lucha contra la explotación infantil en línea. El informe menciona iniciativas como la Alianza Global para poner fin a la violencia contra los niños (EVAC) y la red ECPAT, que están trabajando en varios países de la región (UIT, 2021). Sin embargo, se necesita una mayor coordinación y estandarización de esfuerzos entre los países para abordar la naturaleza transnacional de los delitos en línea contra los NNA.

El análisis también señala la importancia de involucrar a múltiples partes interesadas en el desarrollo e implementación de políticas de protección infantil en línea. Sin embargo, se observa que, con excepción de Costa Rica, la mayoría de los países no han logrado una participación integral de todos los actores relevantes, incluyendo a los propios NNA (UIT, 2021). Esta falta de inclusión podría resultar en políticas que no reflejen adecuadamente las necesidades y realidades de los NNA en el entorno digital.

Un desafío crítico identificado en el estudio es la brecha digital persistente en la región. Como se menciona en el caso de Perú, "a pesar de los esfuerzos del gobierno por desplegar redes de banda ancha en todas las regiones del país, la brecha o carencia o de conectividad (en especial a redes de banda ancha) persiste y se agrava mayormente en las zonas alejadas o dispersas fuera de las ciudades" (UIT, 2021, p. 65). Esta brecha no solo

limita las oportunidades digitales para los NNA, sino que también puede exacerbar las vulnerabilidades existentes.

El informe también destaca la importancia de la educación digital y la alfabetización mediática. Sin embargo, se observa una falta de programas integrales y sostenibles en este ámbito en la mayoría de los países estudiados. Como se señala, "La educación en materia de alfabetización y competencias digitales es uno de los grandes retos que tenemos en la Región" (UIT, 2021, p. 42). Esta brecha en la educación digital podría dejar a los NNA mal equipados para navegar de manera segura en el entorno digital.

Un aspecto crítico que merece mayor atención es la falta de mecanismos efectivos de denuncia y respuesta en casos de abuso o explotación en línea. Aunque algunos países han implementado líneas de ayuda, como se menciona en el caso de Colombia, Costa Rica, Paraguay y Perú (UIT, 2021), es necesario evaluar la eficacia de estos mecanismos y asegurar que sean accesibles y conocidos por todos los NNA.

1.9 Teprotejo Línea de Reporte

TeProtejo es una línea de reporte colombiana que se ha convertido en un modelo innovador para la protección de los NNA en el entorno digital. Esta iniciativa, lanzada por Red Papaz en 2012, representa un enfoque integral para abordar los riesgos en línea que enfrentan los menores. Sin embargo, un análisis crítico revela tanto sus fortalezas como sus limitaciones en el contexto más amplio de la protección infantil en línea.

La principal fortaleza de TeProtejo radica en su enfoque multisectorial. La plataforma involucra a diversas entidades gubernamentales, organizaciones no gubernamentales y empresas privadas en un esfuerzo coordinado para responder a las denuncias de contenido ilegal o perjudicial para los NNA en internet. Este modelo de colaboración es crucial para abordar la naturaleza compleja y transfronteriza de los delitos en línea contra menores.

Un aspecto innovador de TeProtejo es su enfoque en la remoción de contenido ilegal. La plataforma trabaja con proveedores de servicios de internet y plataformas digitales para eliminar contenido perjudicial para los NNA. Este enfoque proactivo es crucial en un entorno digital donde el contenido puede propagarse rápidamente. No obstante, surge la pregunta de cómo se equilibra esta práctica con las preocupaciones sobre la libertad de expresión y la censura en internet.

La accesibilidad de TeProtejo es otro punto fuerte. La plataforma ofrece múltiples canales de denuncia, incluyendo una aplicación móvil, un sitio web y una línea telefónica gratuita. Esta diversidad de opciones aumenta la probabilidad de que los NNA y adultos puedan reportar incidentes de manera oportuna. Sin embargo, es crucial investigar si estos canales son igualmente accesibles para todas las comunidades, especialmente aquellas en áreas rurales o con acceso limitado a internet.

Un aspecto crítico que merece atención es el enfoque de TeProtejo en la prevención y educación. Aunque la plataforma ofrece recursos educativos sobre seguridad en línea, no está claro cuán efectivos son estos materiales en la prevención real de riesgos en línea. Se necesita una evaluación rigurosa del impacto de estos esfuerzos educativos en el comportamiento en línea de los NNA.

La expansión regional de TeProtejo, con su implementación en México, es un desarrollo prometedor. Este modelo podría proporcionar una solución escalable para otros países de América Latina que enfrentan desafíos similares en la protección infantil en línea. Sin embargo, es crucial considerar cómo se adapta este modelo a diferentes contextos culturales, legales y tecnológicos.

Un aspecto que requiere un análisis más profundo es cómo TeProtejo aborda la privacidad y la protección de datos de los denunciantes, especialmente cuando se trata de NNA. Aunque la plataforma permite denuncias anónimas, es importante examinar qué medidas se toman para proteger la identidad de los denunciantes y los datos sensibles relacionados con los casos reportados.

La sostenibilidad del modelo TeProtejo también merece un examen crítico. Aunque cuenta con el apoyo de organizaciones internacionales y empresas privadas, es importante cuestionar cómo se asegura la continuidad y escalabilidad del proyecto a largo plazo, especialmente en un entorno tecnológico en constante evolución.

Otro aspecto para considerar es cómo TeProtejo se integra en el marco más amplio de políticas de protección infantil en Colombia y, por extensión, en América Latina. Aunque la plataforma aborda una necesidad crítica, es importante examinar cómo complementa o se alinea con otras iniciativas gubernamentales y no gubernamentales en el ámbito de la protección infantil.

El modelo de la línea de reporte "Teprotejo" se incluye en la investigación debido a su relevancia y papel clave en la protección de NNA contra la explotación sexual y la pornografía infantil en la región. Este modelo resalta la importancia de contar con mecanismos de denuncia y protección accesibles y confiables para las víctimas y testigos

de estos delitos. Esto es crucial para visibilizar y combatir efectivamente la pornografía infantil en la región, lo que justifica su relevancia en el contexto de esta investigación.

SEGUNDO

LA INVESTIGACIÓN DE HECHOS DE PORNOGRAFÍA INFANTIL

2.1. Las direcciones IP en la investigación del delito de pornografía infantil

La globalización y el avance de las tecnologías de la información y comunicación (TIC) han transformado el mundo, permitiendo cruzar fronteras, disminuir los tiempos de respuesta y mejorar la comunicación efectiva y eficiente. Sin embargo, estas innovaciones también han creado nuevas oportunidades para las organizaciones delictivas, las cuales aprovechan la mayor anonimidad y alcance que ofrece el ciberespacio para realizar actividades criminales sin ser detectados fácilmente.

El ciberespacio, un espacio digital donde las personas interactúan, comparten información y realizan diversas actividades en línea, ha cambiado las dinámicas de las relaciones económicas, políticas, sociales y personales (Barrio, 2018). Este término, acuñado por primera vez en la novela de ciencia ficción *Neuromancer* de William Gibson (1984), se refiere a un mundo virtual paralelo al físico donde se pueden realizar muchas actividades que anteriormente solo eran posibles en el mundo real (Scotti, 2016).

Por lo que, la investigación de delitos en el ciberespacio difiere significativamente de la realizada en el mundo físico. En lugar de buscar armas, balas o manchas de sangre, los investigadores se enfocan en dispositivos electrónicos, informáticos, de almacenamiento óptico, y routers. En este contexto, las direcciones IP juegan un papel crucial en la investigación de delitos de pornografía infantil.

Una dirección IP es un conjunto único de números y letras asignado a cada dispositivo conectado a una red de Internet. Funciona como una dirección postal digital que permite la identificación y comunicación entre dispositivos a través de Internet (García, 2023). En investigaciones de pornografía infantil, las direcciones IP son esenciales para rastrear a los perpetradores, identificar a los usuarios que comparten o descargan material ilegal y monitorear el flujo de este material a través de la red. La IP se convierte así en una pista clave para localizar al dispositivo y a la persona responsable del ciberdelito.

Investigar delitos penales en Internet no solo implica identificar la dirección IP, sino también concretar la identidad del usuario del sistema informático asociado a dicha IP (Miró, 2012). En otras palabras, se trata de identificar de manera anónima a la persona detrás de la red. Aunque el ciberdelito es cometido por una persona específica, solo se muestra en Internet una representación virtual del autor (la dirección IP), que debe ser vinculada a la persona física que cometió la acción.

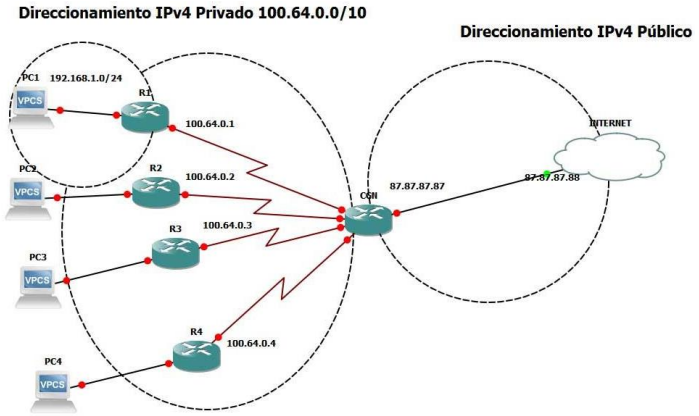
Las direcciones IP se agrupan en varias clases: A, B, C, D y E. Los gobiernos y grandes empresas suelen usar direcciones de clase A, mientras que las medianas empresas utilizan clase B y los usuarios normales, clase C. Las direcciones de clase D son para multidifusión, y las de clase E, para investigación (Méndez Ávila, 2011). Sin embargo, la distribución de direcciones IP no es equitativa, y la demanda de direcciones IPv4 supera la oferta disponible.

Para mitigar esta escasez, los proveedores de servicios de Internet utilizan la técnica CG-NAT (traducción de direcciones de red de nivel de consumidor), que permite que varios usuarios compartan una única dirección IP pública al asignarles direcciones IPv4 privadas simultáneamente (Huawei, 2020). Aunque esto soluciona temporalmente el problema de escasez, también puede complicar la identificación de usuarios específicos en investigaciones criminales.

Las direcciones IPv6, asignadas por LACNIC para América Latina y el Caribe, ofrecen una solución a la escasez de IPv4. Las direcciones IPv6 utilizan 128 bits, proporcionando una cantidad casi ilimitada de direcciones únicas, lo que sugiere que la migración a IPv6 podría resolver la excesiva demanda de direcciones IP (LACNIC, s.f.).

La pandemia de COVID-19 aceleró el uso de las TIC, tanto por parte de organizaciones legales como criminales. La recesión económica mundial y el aumento del desempleo, la pobreza y la desigualdad han incrementado las actividades ilegales en el ciberespacio. El FMI pronosticó una caída del PIB mundial del 3% en 2020, con América Latina siendo una de las regiones más afectadas (Iazzetta, 2020).

Figura 2 ***Protocolo IPv4***



Nota. Adaptado de Protocolo IPv4 [Imagen], Azadsl zone, (2024). Qué es CG-NAT y por qué compartes la IP pública.

2.2 Tipos de internet: clear web, deep web y dark web

El análisis de los diferentes tipos de internet: clear web, deep web y dark web y su relación con los delitos de pornografía infantil revela una compleja interacción entre la tecnología, la criminalidad y los desafíos de la aplicación de la ley. Este estudio crítico examina cómo estas capas de internet facilitan diversos grados de anonimato y accesibilidad, influyendo en la comisión y la investigación de delitos contra menores.

La clear web, también conocida como surface web, representa la parte de internet indexada por motores de búsqueda convencionales. Según Bergman (2001), esta capa constituye solo alrededor del 4% del contenido total de internet. Aunque la clear web es el espacio más familiar para la mayoría de los usuarios, no está exenta de actividades ilícitas, incluyendo la distribución de material de abuso sexual infantil (MASI). Sin embargo, la relativa facilidad de rastreo en esta capa hace que los delincuentes sofisticados tiendan a evitarla para actividades ilegales graves.

La deep web, por otro lado, abarca el contenido no indexado por los motores de búsqueda estándar. Weimann (2016) estima que la deep web es 400-500 veces más grande que la clear web. Esta capa incluye bases de datos privadas, intranets corporativas y otros contenidos protegidos por contraseñas. Aunque la deep web no es inherentemente ilegal, su naturaleza no indexada proporciona un grado de privacidad que puede ser explotado por actores malintencionados.

La dark web, un subconjunto de la deep web, requiere software especial como Tor para acceder. Según un estudio de Intelliagg (2015), la dark web representa solo el 0.01%

del contenido de internet. Sin embargo, este pequeño segmento es conocido por albergar y comercializar una variedad de productos y servicios ilícitos, incluida la distribución de MASI, cuya transacción se la realiza por intermedio de criptomonedas. La dark web ofrece un alto grado de anonimato, lo que la convierte en un refugio atractivo para los ciberdelincuentes.

El problema de la pornografía infantil en la dark web es particularmente preocupante. Un informe de la Internet Watch Foundation (2019) reveló que el 32% del MASI detectado estaba alojado en servicios de alojamiento dark web. Este alto porcentaje subraya la preferencia de los delincuentes por esta capa de internet debido a su capacidad para evadir la detección.

La naturaleza encriptada y anónima de la dark web plantea desafíos significativos para la investigación y el enjuiciamiento. Como señala Europol (2020), "la sofisticación tecnológica de los delincuentes que operan en la dark web a menudo supera la capacidad de las fuerzas del orden" (p. 24). Esta brecha tecnológica dificulta la identificación y el rastreo de los perpetradores.

Sin embargo, es crucial cuestionar la narrativa predominante de que la dark web es impenetrable para las fuerzas del orden. Investigaciones recientes, como las de Jardine (2018), sugieren que las características técnicas que hacen que la dark web sea atractiva para los delincuentes también pueden facilitar su vigilancia. Por ejemplo, el número limitado de nodos de salida en la red Tor puede, en teoría, ser monitoreado para detectar actividades sospechosas.

La falta de investigación efectiva en la dark web no se debe únicamente a obstáculos técnicos, sino también a limitaciones legales y de recursos. Muchas jurisdicciones carecen de marcos legales adecuados para abordar los delitos cibernéticos en la dark web. Además, la naturaleza transnacional de estos delitos complica aún más la aplicación de la ley, requiriendo una cooperación internacional que a menudo es lenta y burocrática.

Es importante notar que, aunque la dark web facilita la distribución de MASI, la producción inicial de este material a menudo ocurre en el mundo físico o se comparte inicialmente a través de plataformas en la clear web. Un estudio de UNICEF (2020) encontró que las aplicaciones de mensajería y las redes sociales convencionales siguen siendo puntos de entrada comunes para la explotación sexual de menores. Esto sugiere que un enfoque integral para combatir la pornografía infantil debe abordar todas las capas de internet, no solo la dark web.

La creciente sofisticación de las herramientas de anonimización y encriptación plantea nuevos desafíos. Por ejemplo, el uso de criptomonedas para transacciones ilegales en la dark web dificulta el seguimiento del flujo de dinero, una técnica tradicional en las investigaciones de delitos financieros. Según un informe de Chainalysis (2021), las transacciones de criptomonedas relacionadas con MASI en la dark web aumentaron un 32% en 2020 en comparación con el año anterior.

Sin embargo, también están surgiendo nuevas tecnologías y técnicas de investigación. El uso de inteligencia artificial y aprendizaje automático para detectar y clasificar MASI está mostrando resultados prometedores. Un estudio de Westlake et al. (2017) demostró que los algoritmos de IA pueden identificar MASI con una precisión del 94%, superando a los métodos manuales tradicionales.

La colaboración entre las fuerzas del orden y las empresas tecnológicas es crucial para abordar este problema. Iniciativas como el Proyecto Arachnid, desarrollado por el Centro Canadiense para la Protección de la Infancia, utilizan tecnología de rastreo automatizado para detectar MASI en todas las capas de internet, incluida la dark web. Sin embargo, estas colaboraciones a menudo se ven obstaculizadas por preocupaciones sobre la privacidad y la vigilancia gubernamental.

Es importante considerar también el impacto psicológico en los investigadores que se dedican a combatir el MASI en la dark web. Un estudio de Bourke y Craun (2014) encontró altas tasas de estrés traumático secundario entre los investigadores de delitos cibernéticos contra menores. Esto subraya la necesidad de apoyo psicológico y rotación de personal en estas unidades especializadas.

La educación y la prevención juegan un papel crucial en la lucha contra el MASI en todas las capas de internet. Programas de alfabetización digital que enseñen a los menores sobre los riesgos en línea y cómo protegerse es esencial. Sin embargo, como argumenta Livingstone (2019), estos programas deben equilibrar la protección con el empoderamiento digital, reconociendo los beneficios positivos de la participación en línea para los jóvenes.

El debate sobre el cifrado de extremo a extremo en plataformas de mensajería populares añade otra capa de complejidad a este problema. Mientras que el cifrado protege la privacidad de los usuarios, también puede obstaculizar la detección de MASI. Este dilema plantea preguntas éticas sobre el equilibrio entre la privacidad individual y la seguridad pública.

La respuesta legal a la pornografía infantil en la dark web también merece un examen crítico. Muchas jurisdicciones han endurecido las penas para los delitos relacionados con MASI, pero la efectividad de este enfoque punitivo es cuestionable. Estudios como el de Wolak et al. (2014) sugieren que el aumento de las penas no necesariamente disuade a los delincuentes, especialmente en el contexto del anonimato percibido de la dark web.

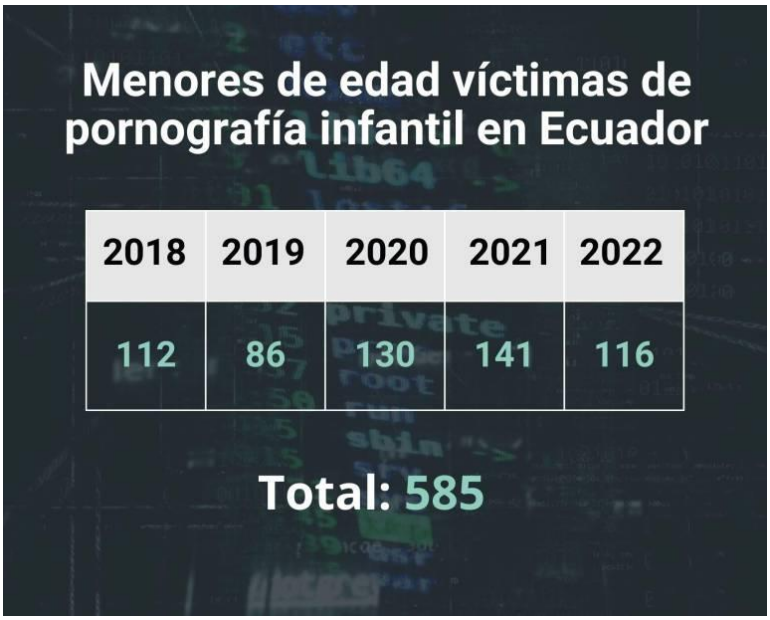
Es crucial reconocer que la lucha contra el MASI en la dark web no es solo un desafío tecnológico, sino también social y económico. La pobreza, la desigualdad y la falta de educación contribuyen a la vulnerabilidad de los menores a la explotación sexual. Abordar estas causas fundamentales es tan importante como mejorar las capacidades de investigación cibernética.

2.3. Dificultades en la investigación de la pornografía infantil

La lucha contra la pornografía infantil en Ecuador presenta una serie de desafíos complejos que reflejan tanto las peculiaridades del contexto nacional como las dificultades globales en la era digital. Este análisis examina críticamente estos retos, cuestionando los enfoques actuales y proponiendo nuevas perspectivas para abordar este problema urgente en el contexto ecuatoriano.

Un aspecto crítico que requiere un examen más profundo es la alarmante subestimación de la magnitud del problema en Ecuador. Según los datos presentados por Hidalgo (2023), la Fiscalía registró 585 casos de pornografía infantil entre 2018 y 2022. Sin embargo, Childfund Ecuador advierte que estas cifras representan apenas una fracción del problema real, estimando que solo uno de cada diez casos se denuncia.

Figura 3 ***Número de víctimas de pornografía infantil***



Nota. Adaptado de Datos del Sistema Integrado de Actuaciones Fiscales (SIAF) [Foto: Ilustración], por Hidalgo, (2023), Pornografía infantil en Ecuador: niños son acechados por redes sociales o incluso los propios familiares los agreden.

Esta discrepancia plantea preguntas fundamentales sobre la eficacia del sistema de protección infantil y justicia penal en Ecuador. ¿Por qué existe esta reticencia generalizada a denunciar? ¿Es un reflejo de la desconfianza en las instituciones ecuatorianas, el temor a la estigmatización social, o quizás una señal de que las vías de denuncia no son lo suficientemente accesibles o seguras en el contexto local?

La subnotificación masiva sugiere que las estrategias actuales para combatir la pornografía infantil en Ecuador podrían estar basadas en una comprensión fundamentalmente sesgada de la escala y naturaleza del problema. Es crucial cuestionar cómo este subregistro afecta la asignación de recursos y la formulación de políticas públicas en el país.

Las autoridades ecuatorianas encargadas de investigar la pornografía infantil enfrentan significativas limitaciones tecnológicas. Según las entrevistas realizadas con expertos fiscales y policiales nacionales e internacionales, uno de los principales obstáculos es la dificultad para identificar las direcciones IP de los perpetradores.

Esta situación plantea interrogantes críticas sobre la capacidad tecnológica de las instituciones de justicia ecuatorianas. ¿Cómo puede Ecuador cerrar la brecha tecnológica entre sus fuerzas del orden y los delincuentes cibernéticos, considerando las limitaciones presupuestarias del país? ¿Qué estrategias innovadoras y costo-efectivas podrían implementarse para mejorar las capacidades de investigación digital?

El caso legal de Yahoo! en Francia, descrito por Puga (2019), ilustra los desafíos jurisdiccionales en el ámbito digital. Aunque este caso no ocurrió en Ecuador, plantea preguntas relevantes para el contexto ecuatoriano: ¿Cómo puede un país en desarrollo como Ecuador hacer valer su jurisdicción frente a gigantes tecnológicos multinacionales? ¿Qué estrategias legales y diplomáticas puede adoptar Ecuador para proteger a sus ciudadanos en el ciberespacio?

Bouyssou (2015) destaca la inadecuación de las leyes nacionales frente a la naturaleza aterritorial del ciberespacio. En el contexto ecuatoriano, esto plantea la necesidad de una revisión crítica del marco legal existente. ¿Están las leyes ecuatorianas actuales equipadas para abordar la complejidad de los delitos cibernéticos contra menores? ¿Cómo puede Ecuador armonizar su legislación con los estándares internacionales sin comprometer sus valores y prioridades nacionales?

Además, la falta de una Red 24/7 en los términos del artículo 35 del Convenio de Budapest, mencionada en el texto, subraya la necesidad de mejorar la cooperación internacional. ¿Cómo puede Ecuador fortalecer sus lazos de cooperación internacional en la lucha contra la pornografía infantil, considerando sus recursos limitados y su posición geopolítica?

Los desafíos en la investigación de la pornografía infantil en Ecuador son complejos y multifacéticos, pero no insuperables. Para avanzar, Ecuador necesita un cambio de paradigma que vaya más allá de las soluciones incrementales y aborde las raíces sistémicas del problema en su contexto específico.

2.4 Análisis de entrevista

El teniente coronel Gonzalo García, jefe de la Unidad Nacional de Ciberdelitos de la Policía Nacional del Ecuador, fue entrevistado sobre las dificultades para investigar el delito de pornografía infantil en el país. Durante sus 27 años en la institución policial, 16 de los cuales han sido en el área investigativa y 2 años y medio como jefe de la Unidad de Ciberdelitos, ha enfrentado varios desafíos en este ámbito.

Uno de los principales problemas es la falta de colaboración de los proveedores de servicios de internet (ISP) para entregar información que permita identificar a los responsables, como las direcciones IP. También se requiere que las redes sociales y proveedores de correo electrónico entreguen datos de los suscriptores, siempre con la debida autorización judicial. Aunque existen buenas leyes contra la pornografía infantil

en Ecuador, hace falta mayor conocimiento por parte de las víctimas sobre cómo denunciar. Además, a veces se normaliza este delito cuando los victimarios son del entorno cercano de los menores. Se necesita una alfabetización digital para que la ciudadanía sepa usar adecuadamente la tecnología.

La cooperación internacional es clave al tratarse de delitos transnacionales. Ecuador está próximo a adherirse al Convenio de Budapest, lo que facilitará la coordinación con otros países. Sin embargo, el acceso a tecnología actualizada por parte de las autoridades es todavía limitado debido a los altos costos. Es importante mejorar la articulación entre entidades públicas, privadas y academia. Se requieren políticas públicas enfocadas en prevención, incluyendo estos temas en mallas curriculares y fomentando nuevas carreras técnicas. Una lección aprendida es evitar la revictimización de los menores durante las investigaciones y procesos judiciales.

Por otro lado, la entrevista a Silvana Paola Solís Cabrera, fiscal de delincuencia organizada transnacional e internacional en Quito. En cuanto a la prevalencia del problema, la fiscal indica que Ecuador tiene un convenio con la embajada de Estados Unidos para trabajar con la unidad de ciberdelito. Las denuncias son recibidas por la policía a través de una fundación creada por el Congreso de EE.UU. que tiene un acuerdo con el Ministerio del Interior. Sin embargo, la problemática es que no siempre la ciudadanía tiene el conocimiento adecuado para denunciar y proseguir con los casos.

Las principales dificultades que enfrenta la jurisprudencia ecuatoriana son no ser parte de la Convención de Budapest, lo cual ayudaría en el tema investigativo a nivel internacional, y el problema con las direcciones IP versión 4, que están caducas y dificultan la investigación al designar una misma IP a varios usuarios. Se debería pasar a la versión IP 6. En cuanto a la efectividad de las leyes, Ecuador tiene una ley sólida con los artículos 103 y 104 del COIP, la Constitución y el Código de la Niñez y Adolescencia. Pero ser parte de la Convención de Budapest ayudaría mucho en la investigación.

Los principales desafíos técnicos son las IP versión 4 caducas que no brindan la información necesaria. Además, hay 3 niveles de conocimiento de los infractores, desde los que usan redes sociales comunes hasta los que usan redes oscuras y códigos, lo que dificulta la detección. La cooperación internacional juega un papel importante a través del convenio con la embajada americana, la organización NCMEC que canaliza denuncias, y el apoyo de la unidad policial HSI en capacitación y herramientas tecnológicas. Pero sería beneficioso que Ecuador forme parte de la Convención de Budapest.

Para mejorar la identificación y persecución de los responsables, se requiere capacitación no solo a la Fiscalía y policía, sino también a los jueces para que conozcan sobre IP, tecnologías usadas por los delincuentes y tengan mayor sensibilidad sobre el interés superior del niño al dictar medidas. La coordinación entre autoridades gubernamentales, ONG y sector privado puede mejorarse con mesas de trabajo donde cada institución exprese sus necesidades, por ejemplo que el Ministerio de Telecomunicaciones exija a las operadoras privadas la migración a IP versión 6.

Como políticas públicas, se requieren campañas comunicacionales a la ciudadanía sobre los riesgos del uso de tecnología por menores y el peligro detrás de las redes sociales. Las lecciones aprendidas de casos anteriores muestran que si bien hay un buen trabajo investigativo, se requiere el cambio a IP versión 6, mayor información a la ciudadanía y capacitación a la judicatura, tomando en cuenta el interés superior del niño por sobre formalidades como notificaciones que pondrían en riesgo la evidencia digital.

Miguel Salazar, investigador criminal de la oficina de investigaciones del Departamento de Seguridad Nacional en la embajada de Estados Unidos en Quito, junto con sus colegas Israel Loor y Ricardo Ramírez, mencionan:

En los últimos 5 años, Miguel se ha especializado en el combate contra la explotación infantil en línea, también conocido como material de abuso sexual infantil. Él considera que este delito ha tomado mucho interés en la sociedad ecuatoriana en los últimos 3 años, dejando de ser visto como un crimen sin víctimas. Sin embargo, Israel señala que aún hay cifras ocultas, especialmente en regiones como Galápagos donde la tasa de denuncias es baja debido a vínculos familiares y falta de involucramiento policial.

Una de las principales dificultades que enfrenta la justicia ecuatoriana es que las investigaciones se basan en direcciones IP versión 4 (dinámicas), que permiten que varios usuarios se conecten a la misma IP el mismo día, dificultando identificar al sospechoso. En contraste, las IP versión 6 (estáticas) permiten saber con nombre y apellido quién contrató el servicio. Esto facilitaría actuar de manera más ágil en la prevención y rescate de víctimas.

Otro desafío técnico es la falta de explotación de dispositivos in situ. Actualmente se incautan los aparatos para ser periciados días después, perdiendo posible evidencia alojada en la nube. Ricardo enfatiza la importancia de explotar los dispositivos en el lugar para tener suficientes indicios para arrestar inmediatamente al sospechoso y evitar que siga victimizando o destruyendo pruebas. Se requieren fiscales, jueces e investigadores especializados que estén al día en temas como criptomonedas y darknet. También se

mencionan iniciativas exitosas como el Sistema de Protección Infantil (SPAI) de Guatemala, que permite agilizar las investigaciones al tener fiscales, policías y peritos trabajando en conjunto y coordinadamente.

La cooperación internacional ha sido clave, especialmente con el NCMEC (National Center for Missing and Exploited Children) de Estados Unidos, que envía miles de reportes de abuso infantil a Ecuador. Además, bajo leyes estadounidenses, las empresas de internet están obligadas a reportar este material ilícito, lo cual facilita las investigaciones. Se busca impulsar legislación similar en Ecuador.

Para mejorar la lucha contra este crimen, los entrevistados recomiendan:

- Adoptar el uso de IP versión 6 a nivel nacional
- Permitir la explotación de dispositivos in situ
- Reformar la ley de notificación y fortalecer la reserva investigativa
- Adhesión al Convenio de Budapest para facilitar cooperación internacional
- Crear un registro público de ofensores sexuales
- Restricción domiciliaria para convictos (no vivir cerca de parques o escuelas)
- Campañas de prevención como "I-Guardian" de HSI
- Reparación integral a víctimas mediante extinción de dominio a bienes de abusadores
- Cambiar el término "pornografía infantil" por "material de abuso sexual infantil"

Por otra parte, José María Gómez de la Torre, ingeniero informático con experiencia en ciberseguridad. Ha trabajado en la respuesta a incidentes relacionados con la pornografía infantil en línea. Quien ha sido parte de ECUSER y Jorge Guerrón, Jorge Guerrón es un ingeniero en sistemas especializado en ciberseguridad. Ha desarrollado su carrera apoyando a instituciones de justicia en la investigación de delitos cibernéticos, trabajando como perito informático forense para la Función Judicial, calificado por el Consejo de la Judicatura. Su experiencia incluye el apoyo a equipos de criminalística y Policía Judicial en la investigación de delitos contra niños, niñas y adolescentes.

Ambos entrevistados coinciden en que la magnitud del problema de pornografía infantil en Ecuador es considerable y probablemente mayor de lo que reflejan las estadísticas oficiales. Señalan la existencia de redes organizadas que comparten material

ilícito a través de diversas plataformas digitales, incluyendo redes sociales y aplicaciones de mensajería.

En cuanto al marco legal, se ha observado una evolución reciente. José María Gómez de la Torre menciona que hasta hace poco, estos delitos no estaban bien identificados en la legislación ecuatoriana. La adhesión al Convenio de Budapest, mencionada por ambos, ha iniciado un proceso de adecuación normativa, lo que sugiere una mejora en la capacidad legal para abordar estos crímenes.

Una de las principales debilidades identificadas por ambos entrevistados es la falta de recursos humanos especializados y capacitados. Existe una escasez de personal en la policía, fiscalía y judicatura para investigar y procesar estos casos complejos. Además, la alta rotación del personal entrenado agrava este problema, dificultando la acumulación de experiencia y conocimientos especializados.

Los desafíos tecnológicos representan un obstáculo significativo en la investigación de estos delitos. Ambos entrevistados destacan la falta de herramientas y licencias de software adecuadas para el análisis forense digital, la complejidad en el rastreo debido al uso de VPNs y técnicas de ocultamiento, y las limitaciones en el uso de direcciones IP (tanto IPv4 como IPv6) para identificar a los perpetradores.

La cooperación internacional se presenta como un elemento crucial. Aunque se han logrado mejoras en los últimos años, ambos entrevistados señalan que aún existe un amplio margen para fortalecer esta colaboración. La naturaleza transnacional de estos delitos hace que la coordinación entre países sea fundamental para una investigación efectiva.

Tanto Gómez de la Torre como Guerrón destacan la complejidad adicional que representa la dark web para las investigaciones, donde se comercializa material de abuso infantil y se llevan a cabo actividades de tráfico de menores. Esto subraya la necesidad de desarrollar capacidades especializadas para operar en estos entornos digitales ocultos.

Ambos entrevistados consideran importante y potencialmente eficaz la figura del agente encubierto informático para infiltrarse en redes de delincuentes. Esta estrategia podría proporcionar información valiosa sobre el modus operandi de los criminales y ayudar a desmantelar redes organizadas.

El análisis también revela la necesidad de fortalecer las políticas públicas enfocadas en la educación y prevención, así como en mejorar los canales de denuncia y la protección de las víctimas. Estas medidas son fundamentales para abordar el problema de manera integral, más allá de la persecución penal.

Finalmente, ambos entrevistados enfatizan la importancia de documentar adecuadamente los casos y procesos de investigación para aprender de experiencias pasadas y mejorar continuamente las técnicas investigativas. Este enfoque de aprendizaje continuo es crucial para adaptarse a las rápidas evoluciones en las tácticas de los delincuentes y las tecnologías utilizadas.

2.4.1 Triangulación de Datos

Desde la perspectiva de las autoridades policiales, encabezadas por el teniente coronel Gonzalo García, se destacan desafíos como la falta de colaboración de los proveedores de servicios de internet, la necesidad de mayor alfabetización digital ciudadana y las limitaciones en el acceso a tecnología actualizada. Estos factores dificultan significativamente la identificación y persecución de los delincuentes.

Por su parte, la visión de los fiscales y juristas, representada por Silvana Paola Solís Cabrera, enfatiza los problemas técnicos y legales. Se señala como un obstáculo importante el uso de direcciones IP versión 4, que complica la identificación precisa de usuarios. Además, se subraya la urgencia de que Ecuador se adhiera a la Convención de Budapest para mejorar la cooperación internacional en investigaciones. La capacitación especializada de todos los actores del sistema judicial, incluyendo jueces, se considera crucial para abordar eficazmente estos delitos tecnológicos.

Desde la perspectiva de los expertos técnicos, como José María Gómez de la Torre y Jorge Guerrón, se resalta la escasez de recursos humanos especializados en todas las instancias involucradas. También se menciona la falta de herramientas y software adecuados para el análisis forense digital. Estos expertos hacen hincapié en la complejidad añadida por el uso de la Dark Web en estos delitos y proponen fortalecer la figura del agente encubierto informático como una estrategia potencialmente efectiva.

La triangulación revela varios puntos de convergencia entre las diferentes perspectivas. Todos los expertos coinciden en que las limitaciones tecnológicas, especialmente el uso de direcciones IP versión 4, representan un obstáculo significativo. También hay consenso sobre la importancia de la cooperación internacional, particularmente la adhesión al Convenio de Budapest. La necesidad de capacitación especializada y continua para todos los actores involucrados es otro punto de acuerdo, así

como la urgencia de actualizar leyes y procedimientos para adaptarse al entorno digital cambiante.

Sin embargo, también se observan algunas divergencias o énfasis diferentes entre los grupos. Mientras las autoridades policiales se centran en la falta de tecnología actualizada, los expertos técnicos enfatizan más la escasez de personal especializado. Los fiscales priorizan cambios legales y procedimentales, en tanto que los expertos técnicos se enfocan en herramientas de análisis forense y capacidades de investigación en la dark web. Además, el rol del sector privado, particularmente la colaboración de los ISP, es más enfatizado por las autoridades policiales que por los otros grupos.

En tal sentido, los datos subrayan la necesidad de un enfoque integral y multidisciplinario para abordar eficazmente el delito de pornografía infantil en Ecuador. La complejidad del problema requiere la colaboración estrecha entre diferentes sectores, la actualización constante de capacidades técnicas y legales, y un esfuerzo sostenido en educación y prevención. Solo mediante la combinación de estos elementos se podrá mejorar significativamente la capacidad de investigación y persecución de este grave delito, protegiendo así a los NNA en el entorno digital.

2.5. Reportes de casos de pornografía infantil por intermedio de National Center For Missing &Exploited Children (NECMEC)

Figura 4 ***National Center For Missing &Exploited Children***

Nota. Adaptado de No matter what, we never stop [Fotografía], por National Center For Missing &Exploited Children, sf.

El fenómeno de la pornografía infantil y su difusión en línea representa un desafío global que requiere una respuesta coordinada y efectiva. El National Center for Missing & Exploited Children (NCMEC), fundado en 1984 por John y Revé Walsh, se ha posicionado como una organización clave en la lucha contra la explotación sexual infantil (NCMEC, s.f.). Sin embargo, es preocupante que muchos profesionales del derecho y principalmente administradores de justicia desconozcan la existencia y el alcance de esta organización, lo que podría estar limitando la efectividad de las acciones contra este tipo de delitos.

La creación de CyberTipline en 1998 marcó un hito significativo en la detección y reporte de casos de explotación sexual infantil en línea. Este sistema ha demostrado ser una herramienta valiosa, recibiendo millones de denuncias desde su implementación (NCMEC, s.f.). No obstante, el incremento exponencial de reportes, que alcanzó 21,7 millones en 2020, plantea interrogantes sobre la capacidad de las autoridades para procesar y actuar sobre esta cantidad abrumadora de información.

Es particularmente alarmante el aumento del 28% en los informes de CyberTipline entre 2019 y 2020, así como la duplicación de las denuncias públicas de explotación sexual en línea durante el mismo período (NCMEC, s.f.). Este incremento podría atribuirse a varios factores, incluyendo un mayor uso de internet durante la pandemia de COVID-19, una mayor conciencia pública sobre el problema, o posiblemente un aumento real en la incidencia de estos delitos. Se requiere un análisis más profundo para comprender las causas subyacentes de este fenómeno y desarrollar estrategias de prevención más efectivas.

Figura 5 ***Informas de CyberTipline de los años 2019 y 2020***

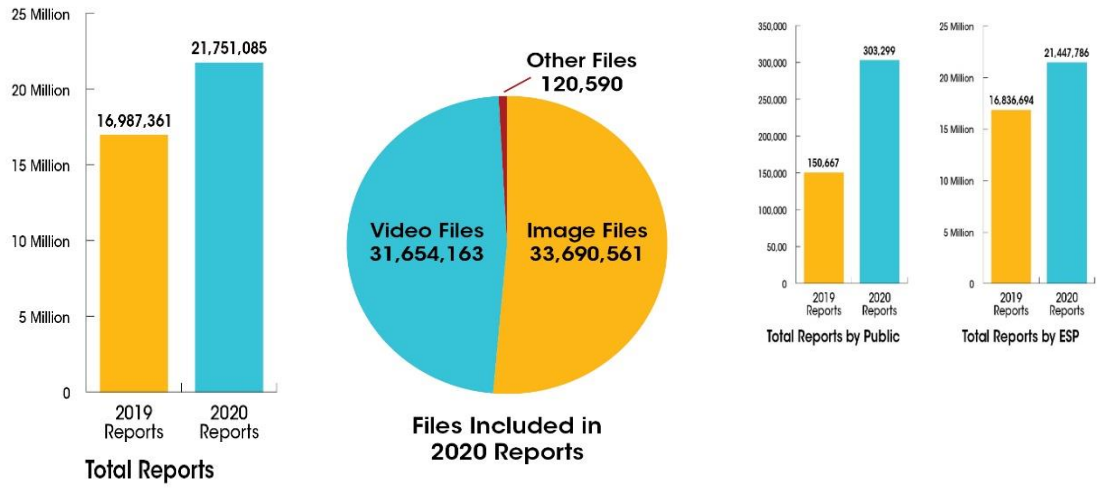
País	Informes año 2019	Informes año 2020
Ecuador	98,669	242,631

Nota. NEMEC, s.f

El caso de Ecuador, donde los reportes de CyberTipline aumentaron de 98,669 en 2019 a 242,631 en 2020, refleja una tendencia preocupante que merece atención especial. Este incremento significativo plantea preguntas sobre la capacidad de la Fiscalía Especializada en Delincuencia Organizada Transnacional e Internacional, La Unidad

Nacional Especializada en Investigación de Ciberdelito de la Fiscalía General del Estado y la Unidad Nacional de Ciberdelitos de la Policía Nacional para manejar eficazmente este volumen de casos. Además, sugiere la necesidad de fortalecer las medidas de protección para NNA en el entorno digital, en consonancia con las garantías establecidas en la Constitución de la República del Ecuador (2008), que prioriza la protección de estos grupos vulnerables.

Figura 6 ***Números de CyberTipline***



Nota. NEMEC, s.f

2.6. Formas de distribución de pornografía infantil en el ciberespacio

Las formas de distribución de pornografía infantil en el ciberespacio han evolucionado de manera alarmante, aprovechando los avances tecnológicos y explotando las vulnerabilidades del entorno digital. Este fenómeno plantea desafíos críticos para la sociedad, las autoridades y los legisladores, quienes se encuentran en una constante carrera contra el tiempo para desarrollar estrategias efectivas de prevención y persecución.

El ciberespacio, con su naturaleza descentralizada y global, ha proporcionado un terreno fértil para la proliferación de material de abuso sexual infantil (MASI). La facilidad de acceso, el anonimato percibido y la rapidez en la transmisión de datos han convertido al internet en un medio preferido para los delincuentes. Sin embargo, es crucial cuestionar si nuestro enfoque actual para combatir este problema es adecuado o si estamos

simplemente reaccionando a las innovaciones de los perpetradores sin abordar las causas fundamentales.

Morillas Fernández (2004) señala la alarmante facilidad con la que se puede acceder a contenido ilegal en línea. Esta observación nos obliga a cuestionar la efectividad de los sistemas de filtrado y control implementados por motores de búsqueda y plataformas en línea. ¿Están estas empresas tecnológicas asumiendo suficiente responsabilidad en la prevención de la distribución de MASI? La naturaleza descentralizada de internet presenta un desafío significativo, ya que el bloqueo de un sitio a menudo resulta en la proliferación de otros, creando un efecto de "hidra" difícil de controlar.

El uso generalizado de tecnologías de anonimización como VPNs, el navegador Tor y la dark web han complicado enormemente la labor de las fuerzas del orden. Esto plantea interrogantes fundamentales sobre la adecuación de las técnicas de investigación tradicionales en este nuevo contexto digital. ¿Están las autoridades suficientemente equipadas y capacitadas para operar eficazmente en estos entornos digitales complejos? Además, surge la pregunta de cómo equilibrar la necesidad de investigar estos delitos con la protección de los derechos de privacidad en línea de los ciudadanos.

Las redes peer-to-peer (P2P) se han convertido en uno de los principales vectores de distribución de MASI, como señala de la Rosa Cortina (2012). La naturaleza descentralizada de estas redes dificulta enormemente la identificación de los responsables, planteando serios desafíos legales y técnicos. Este escenario nos obliga a reconsiderar los marcos legales existentes. ¿Son las leyes actuales adecuadas para abordar los desafíos que presentan estas tecnologías en constante evolución? ¿Cómo podemos adaptar nuestros sistemas legales para ser más ágiles frente a los rápidos cambios tecnológicos?

López (2007) destaca cómo las comunidades virtuales de pedófilos utilizan herramientas tecnológicas avanzadas para mantener su anonimato y evadir la detección. Esta sofisticación tecnológica subraya la necesidad de una constante actualización y adaptación de las estrategias de investigación policial. Sin embargo, cabe preguntarse si esta carrera tecnológica entre delincuentes y autoridades es sostenible a largo plazo. ¿No deberíamos estar enfocándonos también en estrategias de prevención más efectiva y en abordar las causas raíz de la explotación infantil?

El uso de sitios web, grupos de noticias y salas de chat para la distribución de MASI plantea preguntas importantes sobre la responsabilidad de los proveedores de

servicios de internet y las plataformas de redes sociales. ¿Deberían estas empresas asumir un papel más proactivo en la detección y eliminación de contenido ilegal? ¿Cómo podemos fomentar la colaboración entre el sector privado y las autoridades sin comprometer la privacidad de los usuarios legítimos?

La distribución de MASI a través de correo electrónico y mensajería instantánea, aunque menos común debido a los riesgos de detección, sigue siendo una preocupación. Esto plantea interrogantes sobre la efectividad de las técnicas de investigación encubierta y el uso de agentes infiltrados en línea. ¿Cómo podemos mejorar estas estrategias sin cruzar líneas éticas o legales?

Es fundamental reconocer que la lucha contra la distribución de pornografía infantil en el ciberespacio no puede limitarse a medidas reactivas o puramente tecnológicas. Debemos abordar este problema desde una perspectiva más holística, considerando factores sociales, económicos y psicológicos que contribuyen a la explotación infantil. ¿Estamos invirtiendo suficientes recursos en programas de prevención, educación y apoyo a las víctimas?

Además, es crucial examinar críticamente el impacto de nuestras estrategias actuales. ¿Están nuestros esfuerzos para combatir la distribución de MASI en línea teniendo un efecto significativo, o simplemente estamos empujando estas actividades más profundamente en la clandestinidad? ¿Cómo podemos medir de manera efectiva el éxito de nuestras intervenciones?

La cooperación internacional es otro aspecto crucial que merece mayor atención. Dado que la distribución de MASI en el ciberespacio trasciende las fronteras nacionales, ¿cómo podemos mejorar la colaboración entre países para abordar este problema global? ¿Son suficientes los marcos legales internacionales actuales, o necesitamos nuevos acuerdos y protocolos?

2.7 Diferencia entre el SEXTING vs el MASI producido en el marco del crimen organizado transnacional e internacional

La distinción entre SEXTING producidos entre adolescentes en entornos escolares y el MASI generados por el crimen organizado transnacional e internacional es un tema complejo que requiere un análisis crítico y matizado. Esta diferenciación es crucial no solo para comprender la naturaleza diversa de estas actividades, sino también para desarrollar respuestas legales y políticas públicas apropiadas.

En el contexto escolar, la producción de imágenes sexualmente explícitas entre adolescentes a menudo se enmarca dentro del fenómeno del "sexting". Wolak y Finkelhor (2011) definen el sexting como "imágenes sexualmente explícitas producidas por jóvenes menores de 18 años" (p. 2). Este fenómeno, aunque potencialmente dañino, generalmente carece de la intención criminal asociada con la explotación sexual infantil organizada. Sin embargo, es importante notar que las consecuencias legales y sociales pueden ser igualmente graves para los adolescentes involucrados.

Un estudio realizado por Madigan et al. (2018) encontró que aproximadamente uno de cada siete adolescentes envía sexts y uno de cada cuatro los recibe. Estos números subrayan la prevalencia del fenómeno en entornos escolares. Sin embargo, es crucial cuestionar si la respuesta legal actual, que a menudo trata estos casos bajo las mismas leyes diseñadas para combatir la explotación sexual infantil, es apropiada o efectiva.

Por otro lado, la producción de MASI en el marco del crimen organizado transnacional representa una forma sistemática y deliberada de explotación infantil. Según la UNODC (2020), este tipo de delito "implica redes criminales organizadas que operan a través de fronteras nacionales, utilizando tecnologías avanzadas para producir, distribuir y monetizar el MASI" (p. 15). La escala y la sofisticación de estas operaciones las distinguen claramente de los incidentes entre adolescentes.

Un aspecto crítico para considerar es la disparidad en los recursos y métodos utilizados. Mientras que los casos entre adolescentes generalmente involucran tecnologías cotidianas como teléfonos móviles y aplicaciones de mensajería, el crimen organizado emplea técnicas avanzadas de encriptación, redes anónimas como Tor, y criptomonedas para evadir la detección (Europol, 2019). Esta diferencia tecnológica plantea desafíos significativos para las fuerzas del orden y requiere enfoques de investigación radicalmente diferentes.

La motivación detrás de la producción de MASI también difiere significativamente. En el caso de adolescentes, la producción y distribución de este material a menudo está motivada por la exploración sexual, la presión de los pares o la falta de comprensión de las consecuencias (Livingstone & Smith, 2014). En contraste, el crimen organizado está impulsado principalmente por el lucro financiero y opera dentro de una economía ilícita global.

Es crucial examinar críticamente cómo los marcos legales actuales abordan esta distinción. Muchas jurisdicciones aplican las mismas leyes de pornografía infantil tanto a casos de sexting entre adolescentes como a operaciones de crimen organizado. Esto

plantea preguntas éticas y prácticas sobre la proporcionalidad y la eficacia de la respuesta legal. Como argumenta Hasinoff (2015), "criminalizar el sexting consensual entre adolescentes puede tener consecuencias no intencionadas y potencialmente dañinas" (p. 109).

La respuesta internacional a estos delitos también refleja esta falta de diferenciación. El Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (ONU, 2000) no hace distinción entre el sexting producido por adolescentes y el MASI generado por redes criminales. Esta falta de matización en los instrumentos internacionales puede llevar a respuestas desproporcionadas y potencialmente perjudiciales en casos de sexting entre adolescentes.

Un aspecto crítico para considerar es el impacto a largo plazo en las víctimas. Mientras que el sexting producido en entornos escolares puede tener consecuencias psicológicas y sociales significativas para los involucrados, así como ser sometidos a procesos extorsivos que es conocido como la sextorsión, el daño causado por la explotación sistemática del MASI ejecutado por el crimen organizado es a menudo más profundo y duradero. Según un estudio de Canadian Centre for Child Protection (2017), las víctimas de explotación sexual infantil organizada reportan mayores tasas de trastorno de estrés postraumático, depresión y dificultades para formar relaciones saludables en comparación con otros grupos.

La respuesta a estos delitos también debe considerar las diferencias en la escala y el alcance. Los incidentes en entornos escolares tienden a ser localizados y pueden abordarse a través de intervenciones educativas y comunitarias. En contraste, combatir el MASI producido por el crimen organizado requiere una respuesta coordinada a nivel internacional, involucrando cooperación entre agencias de aplicación de la ley, proveedores de servicios de Internet y gobiernos (INTERPOL, 2018).

Es importante cuestionar cómo estas diferencias afectan la prevención y la intervención. Las estrategias de prevención para el sexting entre adolescentes podrían centrarse en la educación sobre ciudadanía digital, alfabetización digital, alfabetización digital mediática y consentimiento, mientras que la prevención del MASI producido por el crimen organizado requiere enfoques más amplios que aborden las causas fundamentales de la explotación infantil, incluyendo la pobreza y la desigualdad social.

Otro aspecto crítico es la reinserción y rehabilitación. Para los adolescentes involucrados en sexting, los programas de intervención y educación pueden ser más

apropiados que las medidas punitivas. En contraste, los perpetradores adultos involucrados en redes de crimen organizado de MASI requieren un enfoque de justicia penal más tradicional, aunque no se debe descartar la importancia de la rehabilitación incluso en estos casos.

La tecnología juega un papel crucial en ambos escenarios, pero de maneras distintas. En el contexto escolar, las plataformas de redes sociales y las aplicaciones de mensajería son los principales vehículos para la distribución de MASI. Esto plantea preguntas sobre la responsabilidad de las empresas tecnológicas en la prevención y detección de este contenido. Por otro lado, el crimen organizado utiliza tecnologías más sofisticadas, incluyendo la dark web y las plataformas P2P, lo que presenta desafíos significativos para la aplicación de la ley y requiere soluciones tecnológicas avanzadas.

El sexting producido entre adolescentes en entornos escolares y el MASI generado por el crimen organizado transnacional representan serias amenazas para el bienestar de los NNA, las diferencias en su naturaleza, escala, motivación e impacto requieren respuestas diferenciadas. Es crucial que los marcos legales, las políticas públicas y las estrategias de intervención reconozcan estas distinciones para abordar eficazmente ambos problemas. Esto implica un enfoque más matizado en la legislación, una mayor inversión en educación y prevención en entornos escolares, y una cooperación internacional más robusta para combatir las redes criminales organizadas. Solo a través de un enfoque que reconozca estas complejidades podremos desarrollar estrategias efectivas para proteger a los NNA en el entorno digital cada vez más complejo y necesario del siglo XXI.

Propuesta de solución

La migración de la tecnología de direcciones IP IPV4 a las direcciones IP IPV6, por parte de los proveedores del servicio de internet o ISP contribuirán a brindar celeridad e incrementar la capacidad de respuesta de la Fiscalía General del Estado y la Policía Nacional, condición necesaria para poder identificar a las personas que se encuentran operando ilícitamente de manera anónima detrás de la red, realizando toda la cadena de producción y comercialización de pornografía infantil o MASI, y con ello desarticular a las estructuras criminales organizadas nacionales y transnacionales dedicadas a este delito.

La colaboración constante con organismos internacionales encargados de reportar, investigar y prevenir el delito de pornografía infantil o MASI. Como NCMEC y

Homeland Security Investigations (HSI) tendientes a adoptar las buenas prácticas materializadas en eventos de capacitación a los operadores de justicia especialmente en las formas de distribución y detección de MASI en el ciberespacio, el rol que desempeña NCMEC, CyberTipline, y la necesidad de la explotación de dispositivos in situ como técnica digital forense, permitiría que todos los actores del proceso penal hablen un mismo idioma y cumplan su rol de manera eficiente.

Todo esto se complementaría con la implementación de una Plataforma de Reporte Nacional en Ecuador, inspiradaen el modelo TeProtejo de Colombia, lo que representaría un avance significativo en la lucha contra la pornografía infantil y otros delitos cibernéticos que afectan a NNA. Esta plataforma se concibe como un sistema integral que facilitaríala denuncia ciudadana anónima por intermedio de un sitio web, una aplicación móvil dedicada, disponible tanto para sistemas iOS como Android y línea telefónica gratuita. Lo que facilitaría la respuesta rápida de las autoridades, adaptándose a las necesidades específicas y al contexto legal y tecnológico del país.

Conclusiones

El delito de pornografía infantil en Ecuador representa un desafío complejo y multifacético que requiere un enfoque integral y coordinado para su prevención, investigación y sanción. La tipificación de este delito ha evolucionado significativamente desde 2005, reflejando un creciente reconocimiento de su gravedad. Sin embargo, persisten debates sobre la terminología adecuada, con una tendencia hacia el uso de términos como "material de abuso sexual infantil" (MASI) para enfatizar la naturaleza abusiva del acto y evitar la normalización implícita en el término "pornografía infantil".

La investigación reveló que las limitaciones tecnológicas, particularmente el uso generalizado de direcciones IPv4 y la técnica CG-NAT, plantean obstáculos significativos para la identificación de perpetradores. La migración a la IPv6 es la solución necesaria, pero su exigencia por parte de los organismos de control de las telecomunicaciones es lenta y desinteresada. Además, el uso creciente de tecnologías de anonimización con IA y Deefake, la proliferación de contenido en la dark web y las plataformas P2P complican aún más los esfuerzos de investigación.

El ciberespacio se relaciona con el delito de pornografía infantil ya que es utilizado para su distribución y en algunos casos para su producción. Verificándose por tanto una relación directa e indirecta con el MASI.

Existe una alarmante discrepancia entre los casos reportados y la estimación real del problema. La sugerencia de que solo uno de cada diez casos se denuncia indica una crisis oculta de proporciones significativas. Este subregistro masivo no solo distorsiona la percepción de la gravedad del problema, sino que también afecta la asignación de recursos y la formulación de políticas efectivas.

La naturaleza transnacional del delito subraya la necesidad crítica de una cooperación internacional más robusta. La adhesión de Ecuador al Convenio de Budapest es un paso positivo, pero la implementación efectiva de sus disposiciones sigue siendo un desafío que solo el paso del tiempo y la ejecución de acciones enfocadas en la protección de los NNA nos dará alguna respuesta. La falta de una Red 24/7, como se establece en el artículo 35 del Convenio, es una deficiencia notable que limita la capacidad de respuesta rápida en casos transfronterizos.

Se identificaron brechas significativas en las capacidades tecnológicas y recursos de las instituciones encargadas de investigar estos delitos. La Fiscalía Especializada en Delincuencia Organizada Transnacional e Internacional, Unidad Nacional Especializada en Investigación de Ciberdelito de la Fiscalía General del Estado, Unidad Nacional de Ciberdelitos de la Policía Nacional y otras entidades relevantes necesitan una actualización urgente en términos de equipamiento, formación, recursos humanos y el acompañamiento tecnológico de los ISP migrando su tecnología de las IPV4 a las IPv6, para hacer frente a la sofisticación creciente de los delincuentes cibernéticos.

Aunque Ecuador ha realizado avances en su marco legal, persisten desafíos en la aplicación efectiva de estas leyes, especialmente en el contexto del ciberespacio. La jurisdicción en casos que involucran plataformas y servicios internacionales sigue siendo un área gris que requiere clarificación, fortalecimiento legal y sobre todo capacitación.

El estudio resalta la importancia crítica de la educación digital y la alfabetización mediática como herramientas preventivas. Sin embargo, se observa una falta de programas integrales y sostenibles en este ámbito, lo que deja a los NNA vulnerables a los riesgos en línea.

Se identifica la necesidad de una mayor colaboración con el sector privado, especialmente con los ISP y plataformas de redes sociales. Su papel en la detección temprana y prevención de la distribución de MASI es crucial, pero requiere un equilibrio cuidadoso con las consideraciones de privacidad y libertad de expresión.

El estudio destaca la importancia de distinguir entre los casos de "sexting" entre adolescentes y la explotación sexual infantil organizada. Esta distinción es crucial para desarrollar respuestas legales y de intervención apropiada y proporcional.

Se subraya la necesidad de un mayor enfoque en el apoyo psicológico y la rehabilitación, tanto para las víctimas como para los investigadores expuestos a este material traumático. Los programas de apoyo e intervención deben ser una parte integral de la respuesta global al problema.

Recomendaciones

La lucha contra la pornografía infantil en Ecuador representa un desafío complejo que requiere un enfoque integral y coordinado. A continuación, se presentan una serie de recomendaciones que abarcan diversas áreas clave para la prevención, investigación y sanción de este delito.

Exigir a los operadores del servicio de internet o ISP por intermedio de la Agencia de Regulación y Control de las Telecomunicaciones migren su tecnología IPV4 a las direcciones IPV6. Con ello contribuirán a brindar celeridad e incrementar la capacidad de respuesta de la Fiscalía Especializada en Delincuencia Organizada Transnacional e Internacional, Unidad Nacional Especializada en Investigación de Ciberdelito de la Fiscalía General del Estado y Unidad Nacional de Ciberdelitos de la Policía Nacional, condición necesaria para poder identificar a las personas que se encuentran operando ilícitamente de manera anónima detrás de la red y desarticular a las estructuras criminales organizadas nacionales y transnacionales dedicadas a este delito.

Fortalecer la legislación y la aplicación de las leyes, Ecuador debe continuar mejorando su marco legal para abordar la pornografía infantil o MASI y otros delitos cibernéticos. Para lo cual es necesaria la capacitación constante a los operadores de justicia, especialmente en las formas de distribución y detección de MASI en el ciberespacio, el rol que desempeña el NCEMEC y los CyberTipline y la necesidad de la explotación de dispositivos in situ como técnica digital forense.

La colaboración constante con organismos internacionales encargados de reportar, investigar y prevenir el delito de pornografía infantil o MASI. Como NCMEC y Homeland Security Investigations (HSI) tendientes a adoptar las buenas prácticas en el ámbito preventivo e investigativo así como el fortalecimiento de la legislación para una aplicación especializada.

Mejorar la capacitación y los recursos de las instituciones encargadas de la investigación de este delito como la Fiscalía Especializada en Delincuencia Organizada Transnacional e Internacional, Unidad Nacional Especializada en la Investigación de Ciberdelitos de la Fiscalía General del Estado y la Unidad Nacional de Ciberdelitos de la Policía Nacional, que necesitan una actualización urgente en términos de equipamiento, formación y recursos humanos para hacer frente a la creciente sofisticación de los delincuentes cibernéticos.

La formación debe incluir aspectos técnicos, éticos y legales, que incluya la puesta en marcha de la figura del agente encubierto informático constante en el artículo 483.1 del COIP. Herramienta jurídica indispensable para la investigación de hechos cometidos en el ciberespacio.

Desarrollar programas de educación digital y alfabetización mediática ya que son herramientas preventivas cruciales. Es necesario implementar programas integrales y sostenibles que eduquen a los NNA sobre la seguridad en línea y cómo reconocer y reportar señales de posibles delitos de abuso sexual en su contra.

Fomentar la colaboración con el sector privado como proveedores de servicios de internet ISP y plataformas digitales, lo que es fundamental para la detección temprana, prevención e investigación de la distribución de material de abuso sexual infantil por intermedio del ciberespacio. Es crucial equilibrar las consideraciones de privacidad y libertad de expresión con la necesidad de proteger a los NNA.

Implementar una Plataforma de Reporte Nacional, inspirada en el modelo TeProtejo de Colombia, la cual representaría un avance significativo en la lucha contra la pornografía infantil y otros delitos cibernéticos que afectan a NNA. Esta plataforma debe incluir múltiples canales de denuncia aplicación móvil, sitio web y una línea telefónica gratuita, lo que permitirá además la integración con autoridades competentes y un sistema de seguimiento para garantizar la respuesta rápida y efectiva.

Desarrollar un sistema de seguimiento y análisis de datos mismos que debe incluirse dentro de la plataforma contando con un riguroso proceso de recopilación y análisis de datos sobre los delitos reportados, las áreas geográficas más afectadas y los resultados de las investigaciones.

Estos datos, debidamente anonimizados, servirán para informar el desarrollo de políticas públicas y estrategias de prevención más efectivas. Además, La plataforma debe ser diseñada para adaptarse a las diferentes realidades culturales y lingüísticas de Ecuador,

garantizando su accesibilidad y relevancia para todos los ciudadanos, independientemente de su origen o ubicación geográfica.

La implementación de estas recomendaciones permitirá a Ecuador fortalecer su capacidad para prevenir, investigar y sancionar el delito de pornografía infantil o MASI y otros delitos cibernéticos que afectan a niños, niñas y adolescentes, protegiendo así a las generaciones futuras.

Bibliografía

Asociación rea. (2021). Términos adecuados y violencia sexual en personas menores de edad. Obtenido de https://www.asociacionrea.org/?s=T%C3%A9rminos+adecuados+y+violencia+sexual+en+personas+menores+de+edad

Azadsl zone. (2024). Qué es CG-NAT y por qué compartes la IP pública [Imagen]

Barrio, M. (2018). Delitos 2.0 Aspectos penales, procesales y deseguridad de los ciberdelitos.

Bergman, M. K. (2001). Documento Técnico: La Web Profunda: Revelando Valor Oculto.

Bouyssou, N. I. (2015). Los delitos de corrupción de menores y pornografía infantil.

Centro Canadiense para la Protección de la Infancia. (2017). Encuesta de Sobrevivientes.

Centro Canadiense para la Protección de la Infancia. (2019). Terminología. https://protectchildren.ca/en/resources-research/terminology/

Chainalysis. (2021). Informe sobre Delitos con Criptomonedas 2021.

Código de la Niñez y Adolescencia. (2003). Prohibiciones relacionadas con el derecho a la dignidad e imagen. Obtenido de https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2014/01/este-es-06-C%C3%93DIGO-DE-LA-NI%C3%91EZ-Y-ADOLESCENCIA-Leyes-conexas.pdf

Código Orgánico Penal . (2014). Título IV - Capítulo Primero.

Consejo Nacional para la Igualdad Intergeneracional. (2020). Política pública por una internet segura para niños, niñas y adolescentes. https://www.igualdad.gob.ec/wp-

content/uploads/downloads/2020/09/pol%C3%ADtica_publica_internet_segura.pdf

Constitución de la República del Ecuador. (2008). Apoyo legal en la protección del menor.

Convención sobre los Derechos del Niño (1990). Obtenido de https://www.igualdad.gob.ec/wp-content/uploads/downloads/2017/11/convencion_derechos_nino.pdf

Convenio sobre cibercriminalidad. (2001). Obtenido de http://documentostics.com/documentos/convenio_cibercriminalidad.pdf

de la Rosa Cortina, J. M. (2012). Delitos de pornografía infantil: Otra vuelta de tuerca. *Diario La Ley*.

Dodge, A. (2018). El testigo digital: El papel de la evidencia digital en las respuestas de la justicia penal a la violencia sexual. Feminist Theory, 19(3), 303-321. https://doi.org/10.1177/1464700117743049

ECPAT Internacional. (2016). Directrices terminológicas para la protección de los niños contra la explotación y el abuso sexual. ECPAT Internacional.

Europol. (2019). Evaluación de Amenazas del Crimen Organizado en Internet (IOCTA) 2019.

Europol. (2020). Evaluación de Amenazas del Crimen Organizado en Internet (IOCTA) 2020.

Gallagher, A. T. (2010). La ley internacional sobre la trata de personas. Cambridge University Press.

García, F. (2023). ¿Qué es una dirección IP? Obtenido de https://www.arsys.es/blog/que-es-una-direccion-ip#Que_es_una_direccion_IP

Gillespie, A. A. (2012). Pornografía infantil: Ley y política. Routledge

Gillespie, A. A. (2018). Pornografía infantil. Information & Communications Technology Law, 27(1), 30-54. https://doi.org/10.1080/13600834.2017.1393932

Hasinoff, A. A. (2015). Pánico por Sexting: Repensando la Criminalización, la Privacidad y el Consentimiento. University of Illinois Press.

Hessick, C. B. (2017). Los límites de la pornografía infantil. Indiana Law Journal, 89(4), 1437-1484.

Hidalgo, K. (2023). Pornografía infantil en Ecuador: niños son acechados por redes sociales o incluso los propios familiares los agreden. *Vistazo*. Obtenido de https://www.vistazo.com/actualidad/nacional/pornografia-infantil-en-ecuador-ninos-son-acechados-por-redes-sociales-o-incluso-los-propios-familiares-los-agreden-YN4852111

Huawei. (2020). ¿Cuántas IP privadas se pueden asignar a una sola IP pública para NAT? Obtenido de https://forum.huawei.com/enterprise/es/%C2%BFcu%C3%A1ntas-ip-privadas-se-pueden-asignar-a-una-sola-ip-p%C3%BAblica-para-nat/thread/667219846259163136-667212881550258176

Iazzetta, M. (2020). Estado, crimen organizado y pandemia por Covid-19. *Temas y Debates*(40), 289-294. Obtenido de http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1853-984X2020000300029

Intelliagg. (2015). Deeplight: Iluminando la Dark Web.

Internet Watch Foundation. (2019). Informe Anual 2019.

INTERPOL. (2018). Estrategia global para combatir la explotación y el abuso sexual infantil en línea.

NTERPOL. (2019). Terminología adecuada. https://www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology

Jardine, E. (2018). Privacidad, censura, violaciones de datos y libertad en Internet: Los impulsores del apoyo y la oposición a las tecnologías de la Dark Web. New Media & Society, 20(8), 2824-2843.

LACNIC. (s,f). Acerca de LACNIC. Obtenido de https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic

Livingstone, S. (2019). EU Kids Online 2020: Resultados de la encuesta de 19 países. EU Kids Online.

Livingstone, S., & Smith, P. K. (2014). Revisión anual de investigación: Daños experimentados por usuarios infantiles de tecnologías en línea y móviles: La naturaleza, prevalencia y gestión de riesgos sexuales y agresivos en la era digital. Journal of Child Psychology and Psychiatry, 55(6), 635-654.

López, A. (2007). La Investigación Policial en Internet; estructuras de cooperación internacional. *Revista de Internet, Derecho y Política, Monográfico, III Congreso Internet, Derecho y Política*.

Madigan, S., Ly, A., Rash, C. L., Van Ouytsel, J., & Temple, J. R. (2018). Prevalencia de múltiples formas de comportamiento de sexting entre los jóvenes: una revisión sistemática y meta-análisis. JAMA Pediatrics, 172(4), 327-335.

Méndez Ávila, D. L. (2011). nvestigación y elaboración de un instructivo sobre las herramientas hacker más utilizadas en el ámbito informático. Obtenido de https://repositorio.uisrael.edu.ec/bitstream/47000/164/1/UISRAEL-EC-SIS-378.242-397.pdf

Miró, F. (2012). El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.

Morillas Fernández, D. L. (2004). Los delitos de pornografía infantil en el derecho comparado. *Cuadernos de política Criminal*, 31-80.

National Center For Missing & Exploited Children. (s.f.). No importa qué, nunca dejamos de buscar [Fotografía].

NECMEC. (s. f). Nuestros comienzos. Obtenido de https://www.missingkids.org/es/footer/about/history

NECMEC. (s.f). Cybertipline. Obtenido de https://www.missingkids.org/es/gethelpnow/cybertipline

ONU. (2000). Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la

pornografía. Obtenido de https://www.ohchr.org/es/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child

Prats, F. M. (2002). El derecho penal ante la pornografía infantil en Internet. In Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet.

Puga, R. (2019). LA EVIDENCIA DIGITAL EN LOS DELITOS DE PORNOGRAFÍA INFANTIL. Obtenido de https://www.dspace.uce.edu.ec/server/api/core/bitstreams/c29fff23-08aa-4d69-9387-776054d0633b/content

Quayle, E., & Cooper, K. (2015). El papel de las imágenes de abuso sexual infantil en las relaciones coercitivas y no coercitivas con adolescentes: Una revisión temática de la literatura. Child & Youth Services, 36(4), 312-328. https://doi.org/10.1080/0145935X.2015.1092840

Quintero, G. (2014). Problemas de la perseguibilidad de los ciberdelitos. In Ciberdelitos: grooming, stalking, bullying, sexting, ciberodio, propiedad intelectual, problemas de perseguibilidad, ciberpornografía infanti.

Rafferty, Y. (2013). Trata de niños y explotación sexual comercial: Una revisión de políticas y programas prometedores de prevención. American Journal of Orthopsychiatry, 83(4), 559-575. https://doi.org/10.1111/ajop.12056

Reformas al Código Penal . (2005). Pornografía infantil .

Salter, M. (2017). Abuso sexual infantil: Ética y evidencia. Child Abuse Review, 26(1), 31-39. https://doi.org/10.1002/car.2443

Sanz Mulas, N. (2009). Pornografía en internet. *Revista Penal*. Obtenido de https://www.academia.edu/93167861/Pornograf%C3%ADa_en_Internet

Scotti, L. B. (2016). impacto de Internet en el mundo jurídico: Una mirada desde el Derecho Internacional Privado. *Foro Jurídico*(15), 178-198.

Svevo-Cianci, K. A., Hart, S. N., & Rubinson, C. (2011). Protegiendo a los niños de la violencia y el maltrato: Un análisis comparativo cualitativo que evalúa la

implementación del Artículo 19 de la CRC de la ONU. Child Abuse & Neglect, 35(10), 1195-1205. https://doi.org/10.1016/j.chiabu.2010.04.006

Taylor, M. (2018). La ética del material de abuso sexual infantil y el internet. En B. Leclerc & E. Savona (Eds.), Prevención del crimen en el siglo XXI (pp. 419-434). Springer.

UNICEF. (2019). Convención sobre los Derechos del Niño: Preguntas frecuentes. https://www.unicef.org/child-rights-convention/frequently-asked-questions

UNICEF. (2020). Acción para poner fin al abuso sexual infantil y la explotación: Una revisión de la evidencia 2020.

UNODC. (2020). Informe global sobre la trata de personas 2020.

Weimann, G. (2016). Migración terrorista hacia la Dark Web. Perspectivas sobre el Terrorismo, 10(3), 40-44.

Westlake, B. G., Bouchard, M., & Frank, R. (2017). Encontrando a los actores clave en las redes de explotación infantil en línea. Política e Internet, 9(2), 206-229.

Wolak, J., & Finkelhor, D. (2011). Sexting: Una tipología. Centro de Investigación de Crímenes contra Niños.

Wolak, J., Finkelhor, D., & Mitchell, K. J. (2014). Tendencias en arrestos por posesión de pornografía infantil: El Tercer Estudio Nacional de Victimización Juvenil en Línea (NJOV-3). Centro de Investigación de Crímenes contra Niños.

Anexos

Entrevista al Teniente Coronel Gonzalo García, jefe de la Unidad Nacional de Ciberdelitos de la Policía Nacional del Ecuador.

Guía de Entrevista

Tema: El delito de pornografía infantil en el Ecuador dificultades investigativas

Objetivos: Determinar la relación del ciberespacio con el delito de pornografía infantil. Evidenciar cómo inciden las direcciones IPV4 en la investigación del delito de pornografía infantil.

Persona Entrevistada: Teniente Coronel Gonzalo García

Persona que realiza la entrevista: Christian Alex Fierro Fierro

Fecha de entrevista: 25-03-2024

Presentación

Soy alumno de la "Maestría en Derecho Penal con Mención en Criminalidad Compleja" de la Universidad de las Américas UDLA. En este contexto como tema de investigación académica estoy investigando sobre "El delito de pornografía infantil en el Ecuador dificultades investigativas".

Solicitud de permiso

Quiero preguntarle antes de iniciar con la entrevista si usted está de acuerdo con que sea grabada, asegurándole que la información será confidencial y se utilizará únicamente con fines académicos. Ante lo cual el entrevistado otorgó el respectivo permiso.

Desarrollo de la entrevista

Preguntas introductorias

Antes de comenzar con la entrevista cuénteme

- **¿Cómo se llama?**

- Soy el Teniente Coronel Gonzalo García, jefe de la Unidad Nacional de Ciberdelitos de la Policía Nacional del Ecuador.
- **¿Cuál es su experiencia profesional en relación con delitos de pornografía infantil?**
- Mi experiencia dentro de la institución policial es de 27 años de servicios, de los cuales aproximadamente 16 años en el eje investigativo de la Policía Nacional y como jefe de la Unidad Nacional de Ciberdelitos, 2 años y medio dentro de este de este periodo de tiempo y específicamente en la Unidad Nacional Ciberdelitos, nosotros contamos con la sección de violencia digital, en la cual investigamos el tema de pornografía infantil.
- **¿Cuál es su opinión sobre la prevalencia y la gravedad del problema en el país?**
- Es un delito que últimamente está teniendo mucha connotación en El País, Principalmente por los casos que Policía Nacional, a través de Fiscalía ha podido detectar y ha sacado a la luz. Uno de los principales problemas en este delito es que no se ponía en conocimiento de las autoridades pertinentes, ya sea por el desconocimiento de las víctimas de cómo poner una denuncia y por el temor.

Preguntas

- **¿Cuáles considera usted que son las principales dificultades que enfrenta la justicia ecuatoriana en la investigación del delito de pornografía infantil?**

  Las dificultades no están direccionadas al tema legal, pero es un poco más del tema técnico, la falta de colaboración de los proveedores de servicio de internet, es decir, de las ISP. Por cuanto estas operadoras de prestadoras de servicio de internet no entregan la información que nosotros como investigadores necesitamos, por ejemplo, al momento de determinar una dirección IP la cual nos

podría ayudar a identificar el domicilio de instalación de esta dirección IP; y, por ende poder saber a nombre de quién se encuentra este servicio, muchas de las operadoras nos contestan indicándonos qué es un pool de IP. Lo que quiere decir que una misma IP está dando servicio a varias personas y domicilios de un mismo sector o también puede ser que no está identificado como tal la IP estática, porque da un servicio de IP dinámicas.

Este es un problema bastante grave que tenemos porque lastimosamente sin esta información, no podemos continuar con la investigación y aquí es cuando la falta de una Política de Estado que obligue a las operadoras de servicio de internet a las ISP, que entreguen esta información o de ser el caso migrar a una nueva tecnología Como sería la IP versión 6.

- **¿Qué herramientas legales considera que son necesarias para fortalecer la capacidad de investigación y persecución de este delito en Ecuador?**

  Una de las principales sería una disposición a nivel País que las todas las proveedoras de servicio de internet redes sociales, correos electrónicos, que se encuentran alojadas en el Ecuador y que tengan almacenado, por ejemplo, información histórica de la IP por lo menos entre 3 a 6 meses. Otra situación importantísima sería que entreguen esta información en tiempos óptimos para la investigación, porque hemos tenido el caso de que muchas operadoras se demoran y muchas veces ni siquiera entregan información.

- **¿Cómo evalúa usted la efectividad de las leyes actuales en la protección de los derechos de los niños y la prevención de la pornografía infantil?**

  Creo tenemos leyes bastante buenas en el tema de pornografía de la de la niñez, de la familia y contra mujeres. Estimo que la normativa sí existe el problema es la falta de conocimiento de la existencia de estas de estas leyes por parte de las

víctimas; y, no dan a conocer la situación que están pasando o están normalizando estas actividades de carácter delictivo, ya que muchas veces los victimarios son gente del propio entorno social de la víctima, padres, hermanos y padrastros, entonces como son parte del círculo cercano familiar, lo normalizan. Muchas veces la mamá vivió lo mismo y ella asume que sus hijas tienen que pasar lo mismo. Entonces este tema de normalización es lo que ha causado un problema bastante serio para que las víctimas no denuncien o no pongan en conocimiento a las autoridades.

- **¿Cuáles son los principales desafíos técnicos y tecnológicos que enfrentan los operadores de justicia al investigar este tipo de delitos en el ciberespacio?**

  Es la falta de asignación de direcciones IP, ya que actualmente el Ecuador ha cerrado la brecha digital. Nosotros tenemos un estudio que indican que casi el 80% de todos Los ciudadanos ecuatorianos ya tienen acceso al internet inclusive desde lugares rurales de, entonces todas estas personas están conectándose al internet, navegando en sus redes sociales, realizando transacciones económicas, etcétera. Y esta esté crecimiento del ecosistema digital tiene que ir de la mano con el acompañamiento técnico para poder obtener información de lo que realizan los usuarios dentro del entorno digital. Aparte de eso, también estimo que hace falta una alfabetización digital. Esto es poder conocer el adecuado uso de las tecnologías lo que permitirá que no sean fácil víctimas de los de los ciberdelincuentes, como la pornografía infantil.

- **¿Qué papel juega la cooperación internacional en la investigación y persecución de la pornografía infantil en Ecuador?**

  Es muy importe la colaboración internacional, tomando en cuenta que estos delitos se los considera como delitos transnacionales. Ya que muchas veces el

victimario puede estar fuera del territorio ecuatoriano y la víctima en el Ecuador. Entonces está esta colaboración entre países es vital. Por eso es necesario que se existan convenios, tratados de comunicación e intercambio de información eficaz. En estos momentos Ecuador está muy próximo a ser parte del convenio de Budapest, los beneficios de esta adhesión será tener un punto de contacto 24/7 lo que permitirá tener esta coordinación directa con nuestros pares de otros países y poder intercambiar información para que la investigación tenga los resultados que se están planificados.

- **¿Cuáles son las medidas más efectivas que podrían implementarse para mejorar la identificación y persecución de los responsables de este delito?**

  Una de las medidas principales yo insisto, es el tema de poner en conocimiento de las autoridades, es decir, denunciar estos delitos que no se queden en el anonimato que se los visualice. Yo creo que partiendo de ahí con la denuncia los actores justicia pueden actuar, pero más allá de eso es la prevención. La prevención es muy importe para que nuestros niños, niñas y adolescentes no sean víctimas de estos delitos. Los niños, los padres, profesores tienen que conocer cómo utilizar adecuadamente el internet, qué subir, qué no subir, qué publicar, qué no publicar, qué postear, qué no postear. Entonces eso es muy importante y lastimosamente en nuestros conciudadanos aún tienen una un desconocimiento de cómo utilizar adecuadamente las tecnologías la información.

- **¿Cuál es su opinión sobre el acceso a tecnología actualizado por parte de las autoridades encargadas de investigar la pornografía infantil?**

  Son herramientas muy costosas en muchos de los casos son sistemas informáticos que no se han venido a implementar en nuestras unidades especializadas de Policía y Fiscalía, entonces sí está aún limitado y aparte de eso el costo de estas

herramientas es alto, ya que por lo general para tener este tipo de herramientas se necesita de licenciamientos, licenciamientos que son anuales en muchos de los casos y que su renovación es costosa. Por eso para esta lucha de la pornografía infantil en línea, se necesita de la inversión del Estado para poder estar a la par con la tecnología de punta que ahora se tiene a nivel mundial.

- **¿Cómo podría mejorarse la coordinación entre las autoridades gubernamentales, las organizaciones no gubernamentales y el sector privado en la lucha contra este delito?**

  Esa es una muy buena pregunta porque lastimosamente cada entidad trabaja como islas, ya sea la parte pública, la parte privada, las autoridades de Justicia trabajan de forma aislada y no nos hemos unido para hacer un solo frente y un solo puño de trabajo en contra de este delito de la pornografía infantil y otros. Entonces, una de las sugerencias es poder articular acciones donde estemos involucrados todos los actores. Se ha dado un paso importante aquí en el Ecuador, al crearse, por ejemplo, el comité nacional de ciberseguridad, donde ya existen algunos entes de todo del Estado que ya somos parte de este de este comité y donde estamos lanzando, por ejemplo, la estrategia nacional, ciberseguridad. Lo que nos permite saber cuál es nuestra misión, qué hacer, cómo actuar. Pero a esto se tendría que sumar, las entidades privadas y la Academia.

- **¿Qué políticas públicas considera que son necesarias para prevenir la pornografía infantil y proteger a los niños en Ecuador?**

  La política pública, tiene que estar enmarcada en el tema de la prevención, por ejemplo, debería existir en las mallas curriculares en escuelas, colegios, universidades, el tema de los ciberdelitos y dentro de esta de la materia las diferentes modalidades. La transversalización de esta de esta materia y que sea

topada en los diferentes niveles escolares. También es importante que exista una política a nivel del Ministerio de Educación, por ejemplo, donde se impulse la creación de nuevas carreras técnicas como la ciberseguridad y ciberdelitos. A nivel de Universidad, posgrados en estos temas con profesionales de alto nivel que sumen a la lucha contra los ciberdelincuentes.

- **¿Cuáles son las lecciones aprendidas de casos anteriores de pornografía infantil en Ecuador y cómo podrían aplicarse para mejorar futuras investigaciones y procesos judiciales?**

  Una de las principales lecciones que hemos podido aprender durante este tiempo es primero, la no revictimización a las niñas, niños y adolescentes, eso es muy importante porque lastimosamente los niños han sufrido este esté atroz delito y muchas veces dentro del proceso investigativo se tiene que nuevamente tomar una versión o hacerse un examen médico legal y valoración psicológica. Entonces todo esto a los niños les afecta, por lo tanto creo que tenemos que ver un mecanismo que en lo menos posible al niño que fue víctima de estos de estos delincuentes se los tenga que estar involucrando dentro del proceso judicial.

  Las entidades encargadas de la investigación de este delito Policía y Fiscalía, cuenten con especialistas que sepan cómo tratar a un menor de edad, desde el nivel psicológico, inclusive saber cómo llevar a una víctima que sufrió esta este percance, que no se vuelva a revictimizar a los niños.

Cierre

Te agradezco por brindarme la entrevista, valoro mucho el tiempo que me ha concedido

Entrevista a la Dra. Silvana Paola Solís Cabrera, Fisca Especializada en la Investigación de Delincuencia Organizada Transnacional e Internacional.

Guía de Entrevista

Tema: El delito de pornografía infantil en el Ecuador dificultades investigativas

Objetivos: Determinar la relación del ciberespacio con el delito de pornografía infantil. Evidenciar cómo inciden las direcciones IPV4 en la investigación del delito de pornografía infantil.

Persona Entrevistada: Dra. Silvana Paola Solís Cabrera

Persona que realiza la entrevista: Christian Alex Fierro Fierro

Fecha de entrevista: 25-03-2024

Presentación

Soy alumno de la "Maestría en Derecho Penal con Mención en Criminalidad Compleja" de la Universidad de las Américas UDLA. En este contexto como tema de investigación académica estoy investigando sobre "El delito de pornografía infantil en el Ecuador dificultades investigativas".

Solicitud de permiso

Quiero preguntarle antes de iniciar con la entrevista si usted está de acuerdo con que sea grabada, asegurándole que la información será confidencial y se utilizará únicamente con fines académicos. Ante lo cual la entrevistada otorgó el respectivo permiso.

Desarrollo de la entrevista

Preguntas introductorias

Antes de comenzar con la entrevista cuénteme

- **¿Cómo se llama?**
- Soy la Dra. Silvana Paola Solís Cabrera, Fisca Especializada en la Investigación de Delincuencia Organizada Transnacional e Internacional.

- **¿Cuál es su experiencia profesional en relación con delitos de pornografía infantil?**
- Es importante indicar que la Fiscalía de Delincuencia Organizada investiga varios delitos y dentro de esos delitos la pornografía infantil que se encuentra en el artículo 103 y 104 del Código Orgánico Integral Penal, investigación que la he realizado aproximadamente 4 años en la en esta Fiscalía.
- **¿Cuál es su opinión sobre la prevalencia y la gravedad del problema en el país?**
- Existe en el País un convenio a nivel internacional con la embajada de Estados Unidos, en donde nosotros trabajamos con la Unidad de Ciberdelito respecto de la pornografía infantil, que cabe indicar, dicho término no es el adecuado, debería llamarse material de abuso sexual infantil MASI porque la pornografía es una especie de diversión adulta de la que refiere este delito, sin embargo, se está tratando de manejarlo de esa manera en las audiencias. Ahora respecto a la prevalencia, yo debo indicar que la institución policial que es quien recibe las denuncias a nivel internacional a través de una institución o de un organismo que fue creado por el Congreso Nacional de Estados Unidos. Y, qué hizo un convenio con el Ecuador a través del Ministerio del interior y quien te recibe las denuncias por parte de redes sociales, es decir, Google, Instagram, Facebook, etcétera.

  La policía recibe estas denuncias y ellos dan a conocer a la Fiscalía a través de los partes policiales correspondiente. Existen varias denuncias, sin embargo, la problemática aquí en el Ecuador, específicamente respecto de las denuncias, es que no siempre las personas tienen el conocimiento adecuado para denunciar, es decir, sí existen las denuncias por parte de la policía, porque a nivel internacional se está generando cuando en territorio digital ecuatoriano se ha estado

descargando MASI, sin embargo, por parte de la ciudadanía no existen denuncias constantes, es decir, son muy pocas las personas que denuncien.

Preguntas

- **¿Cuáles considera usted que son las principales dificultades que enfrenta la justicia ecuatoriana en la investigación del delito de pornografía infantil?**

  Una de las dificultades es no ser parte de la Convención de Budapest. Nosotros tenemos una ley muy segura en el Ecuador respecto a la pornografía infantil o al material de abuso sexual infantil, es decir, tenemos el artículo 103 y el 104 del COIP, que habla tanto de la pornografía con utilización de niños, niñas y adolescentes, y la comercialización también la Constitución que da protección a los menores, el Código Orgánico de la Niñez y Adolescencia. Sin embargo, sí considero importante ser parte de este de esta convención porque ayuda en el tema de investigativo para que nosotros podamos proseguir con las investigaciones de MASIN en el Ecuador.

- **¿Qué herramientas legales considera que son necesarias para fortalecer la capacidad de investigación y persecución de este delito en Ecuador?**

  Herramientas legales las tenemos, sin embargo, tenemos la problemática respecto al tema investigativo con el tema de las IP, porque nosotros trabajamos con una IP versión cuatro, que ya está caduca, deberíamos pasar a la versión IPV6, por qué nosotros tenemos IPS públicas y privadas, estas son aleatorios, o sea dinámicas y estáticas, entonces como eh ya está caduca, es decir, existen hasta 130000 usuarios en una misma IP, y cuando se realiza la petición de información a los ISP generalmente no dan una respuesta adecuada. Porque lamentablemente tienen la misma IP designada a varias personas, entonces dificulta la investigación. No significa que no permite seguir investigando, pero sí es un elemento necesario

para poder continuar con estos delitos y para que sea mucho más efectiva la base legal en una audiencia de juicio donde vamos a demostrar el delito como tal.

- **¿Cómo evalúa usted la efectividad de las leyes actuales en la protección de los derechos de los niños y la prevención de la pornografía infantil?**

  Considero que sí hay una ley sólida aquí en el Ecuador, es decir, existe el Código Orgánico Integral Penal está el artículo 103 y 104, incluso la pena es alta respecto a este tipo de delitos donde se descarga o se comercializa pornografía infantil o más. Tenemos la Constitución de la República artículo 35 y artículo 44, el Código Orgánico de la Niñez y Adolescencia. Sin embargo, es importante que nosotros seamos parte de la Convención de Budapest, porque ayudará mucho en el tema investigativo en el ámbito internacional.

- **¿Cuáles son los principales desafíos técnicos y tecnológicos que enfrentan los operadores de justicia al investigar este tipo de delitos en el ciberespacio?**

  Es importante que nosotros podamos contar con la tecnología de la IP V6 porque la IPV4 está caduca. Es decir, no tenemos la información que deberíamos tener como investigadores, tanto la Policía como la Fiscalía, que somos un equipo técnico. Existen 3 niveles de conocimiento esta actividad ilícita, es decir, el nivel uno que es poco conocimiento tecnológico, que generalmente las personas utilizan el Facebook y el Instagram, Google drive o Google fotos para descargar material de abuso sexual infantil y hacer uso de la misma, sin embargo, también hay un nivel dos en donde ya tienen un poco más de conocimiento técnico respecto a las IP, utilizan estas redes Peer to Peer, que ya que son mucho más difíciles de detectar, no significa que no se las detecte, pero son mucho más complicados y también un tercer nivel que se habla de redes oscuras y códigos. Y se bajan

material de abuso sexual infantil o comercializan y para la Fiscalía se hace mucho más complicado tener la información

- **¿Qué papel juega la cooperación internacional en la investigación y persecución de la pornografía infantil en Ecuador?**

  NCMEC es una de las organización que nos ayudan mucho en la investigación a nivel internacional, porque es a través de esta institución o este sistema que se recibe las denuncias, en donde se determina que a través del territorio digital ecuatoriano se está utilizando o se está descargando, se está comercializando MASI, es decir, sí tenemos colaboración por parte de la embajada americana y por parte de la organización policial HSI tenemos capacitación suficiente, es decir, se está dando herramientas tecnológicas adecuadas para poder trabajar dentro de la investigación. Sin embargo, si es importante, considero el apoyo internacional respecto a la adhesión a la Convención de Budapest.

- **¿Cuáles son las medidas más efectivas que podrían implementarse para mejorar la identificación y persecución de los responsables de este delito?**

  La capacitación de si bien es cierto, la Fiscalía y la Policía tienen una muy buena capacitación y avanzado mucho en la tecnología, es importante que el órgano jurisdiccional, es decir, los jueces, se capaciten respecto al delito para poder ir acorde a lo que se está trabajando. Que ellos conozcan cuáles son las direcciones IP, qué tipo de tecnología utilizan estos delincuentes para poder obtener o descargar, comercializar MASI o incluso utilizar niños, niñas y adolescentes para obtener un rédito económico. Sin embargo, no existe esa capacitación adecuada a las unidades judiciales que impide un poco el trabajo. No, no es que no exista en el Ecuador la colaboración por parte de la judicatura, pero sí es muy difícil hacer entender cuando se pide, sobre todo la reserva judicial respecto de un tema tan

delicado, cuando hay un interés superior que es del niño, por lo tanto sí es necesaria la capacitación adecuada a las entidades jurisdiccionales.

- **¿Cómo podría mejorarse la coordinación entre las autoridades gubernamentales, las organizaciones no gubernamentales y el sector privado en la lucha contra este delito?**

  Considero que es importante realizar mesas de trabajo, porque con eso cada una de las instituciones va a expresar lo que hace por la investigación. Entonces, Fiscalía, por ejemplo, tiene el inconveniente de las IP, por ejemplo, entonces podría el Ministerio de telecomunicaciones tener conocimiento que hace falta que se exija a las entidades privadas ISP para que se puedan pasar de una versión cuatro a una versión 6, que nos ayudaría muchísimo dentro de la investigación, ya que nos van a dar un nombre, un apellido de la persona que está utilizando y que además está descargando, pornografía infantil o material de abuso sexual infantil.

- **¿Qué políticas públicas considera que son necesarias para prevenir la pornografía infantil y proteger a los niños en Ecuador?**

  Por parte de El ministerio de telecomunicaciones debería haber una política pública de información a la ciudadanía, es decir, sobre el riesgo que corren las personas al utilizar la tecnología, los niños sobre todo porque muchas de las personas o muchos de los ciudadanos al no tener ese conocimiento adecuado, obviamente permiten que sus hijos menores de edad utilicen las redes sociales sin tener conocimiento de que puede haber agentes delictivos detrás de esas redes sociales, e incluso con lo que ha avanzado la tecnología como es la inteligencia artificial en donde se pueden crear a avatares o pueden crearse o pueden figurarse niños para tener conexión con menores de edad, O sea, infringir la ley en este caso

y cometer delitos de material de abuso, de descarga o incluso fotografías de los menores de edad.

- **¿Cuáles son las lecciones aprendidas de casos anteriores de pornografía infantil en Ecuador y cómo podrían aplicarse para mejorar futuras investigaciones y procesos judiciales?**

  Creo que es importante nuevamente el tema de las direcciones IP. Esa es una de las cosas que debemos cambiar aquí en el Ecuador ya que no tenemos la información por parte de las redes de telecomunicaciones y obviamente una mayor información a la ciudadanía que el trabajo sea mucho más evidente en conjunto con la judicatura, también porque se requiere capacitación y adicional a eso, creo que una de las problemáticas que también hemos tenido nosotros y que ha sido recurrente es no tomar en consideración este interés superior del niño, o esa empatía hacia este tipo de delitos por parte de la judicatura, porque tenemos muchos inconvenientes al realizar una investigación, que se hace con seguimientos y vigilancias a fin de determinar quién se está descargando comercializando este material de abuso sexual infantil.

  Porque si bien es cierto existe ley expresa respecto a las notificaciones de acuerdo con el artículo 575 del COIP, que para formular cargos en estos casos, nosotros deberíamos notificarles, pero una de las problemáticas al notificar sería que con solo un clic en una computadora se borraría toda la información. En tal virtud se debería tomar en consideración por parte de los jueces, haciendo un razonamiento lógico respecto del tipo de delito que se está investigando, difícilmente nosotros vamos a notificarle a esa persona para que se borre toda la información que existe en el ciberespacio, considerando que es una de las pruebas madre para la Fiscalía,

para demostrar ante un juez o ante un tribunal el delito que se está cometiendo en el Ecuador.

Entonces, se requiere pericias in situ que muchos de los jueces incluso nos han negado y eso creo que considero debe ser cambiado aquí en el Ecuador, para que incluso la gente tenga la seguridad de denunciar y que a nivel internacional seamos vistos como un país que está tratando de evitar este tipo de delitos que van contra los niños, niñas y adolescentes.

Cierre

Te agradezco por brindarme la entrevista, valoro mucho el tiempo que me ha concedido

Entrevista a Miguel Salazar, Ricardo Ramírez e Israel Loor, investigadores criminales para la oficina de investigaciones del Departamento de Seguridad nacional.

Guía de Entrevista

Tema: El delito de pornografía infantil en el Ecuador dificultades investigativas

Objetivos: Determinar la relación del ciberespacio con el delito de pornografía infantil. Evidenciar cómo inciden las direcciones IPV4 en la investigación del delito de pornografía infantil.

Personas Entrevistadas: Miguel Salazar, Ricardo Ramírez e Israel Loor.

Persona que realiza la entrevista: Christian Alex Fierro Fierro

Fecha de entrevista: 28-03-2024

Presentación

Soy alumno de la “Maestría en Derecho Penal con Mención en Criminalidad Compleja” de la Universidad de las Américas UDLA. En este contexto como tema de investigación

académica estoy investigando sobre “El delito de pornografía infantil en el Ecuador dificultades investigativas”.

Solicitud de permiso

Quiero preguntarles antes de iniciar con la entrevista si están de acuerdo con que sea grabada, asegurándoles que la información será confidencial y se utilizará únicamente con fines académicos. Ante lo cual los entrevistados otorgaron el respectivo permiso.

Desarrollo de la entrevista

Preguntas introductorias

Antes de comenzar con la entrevista cuénteme

- **¿Cómo se llama?**
- Miguel Salazar, Ricardo Ramírez e Israel Loor, investigadores criminales para la oficina de investigaciones del Departamento de Seguridad nacional. Aquí en la embajada de Estados Unidos.
- **¿Cuál es su experiencia profesional en relación con delitos de pornografía infantil?**
- Bueno, los últimos 5 años me he venido especializando en el combate contra delitos de trata de personas, específicamente delitos de explotación infantil en línea. Hoy conocidos como material de abuso sexual infantil para el Ecuador y hemos servido como capacitadores para varios otros países en la región en este tema.
- **¿Cuál es su opinión sobre la prevalencia y la gravedad del problema en el país?**
- Bueno, creo que este es un delito que en los últimos 3 años me atrevería a decir que ha tomado mucho interés a nivel de la sociedad. Se han visto muchos casos a nivel de los medios de comunicación donde hemos ya visto casos de explotación

infantil en Línea. Tal vez se lo veía como un delito sin víctimas. Inicialmente no era algo muy común, pero creo que en los últimos 3 años los esfuerzos que hemos venido haciendo conjuntamente con Policía, Fiscalía y todos los entes de la ley han podido ayudarnos a sacar este tema a la luz, es decir, es un delito que tiene una gran prevalencia, no solo aquí en el Ecuador sino a nivel mundial, siendo los Estados Unidos uno de los principales consumidores y productores de este tipo de material, pues el Ecuador no está exento y países en la región tienen esta mismo índice delincuencia en este tipo de delitos.

- Creo que también hay cifras que son muy ocultas y que pasan en regiones muy particulares y como Galápagos, en el cual como son isleños todos se conocen, hay una muy baja tasa de denuncias de esos temas porque todos son familia, parientes, hay afinidad o consanguinidad que ocultan este tipo de delitos y no solo eso a nivel comunitario, sino que a nivel también investigativo. La Policía que va solo por un año allá por ser un régimen especial, no se termina de vincular o involucrar con la sociedad y perseguir estos estas investigaciones. No obstante, la tasa es alta. Siento que todavía hay cifras muy ocultas y me lo han dicho de primera mano compañeros Fiscales de Galápagos.

Preguntas

- **¿Cuáles considera usted que son las principales dificultades que enfrenta la justicia ecuatoriana en la investigación del delito de pornografía infantil?**

  Bueno, principalmente la investigación de este tipo de delitos se basa en lo que son las IP o internet. Que básicamente son las direcciones de conexión del servidor del ISP internet service provider que proporciona esa esa conexión, lo que vemos aquí en las noticias criminales que recibimos específicamente del Centro Nacional de Menores Desaparecidos y Explotados NCMEC por sus siglas en inglés, es que

existe una gran prevalencia de este tipo de denuncias que provienen de direcciones IP versión cuatro muy comúnmente conocidas como IP dinámicas.

Ya que permiten que varios usuarios se conecten a la misma IP en el mismo día en un periodo de tiempo. Esto dificulta el tema investigativo, ya que tenemos que no solamente saber el momento exacto, el día, la hora, el minuto y el segundo, sino que a veces incluso las operadoras de internet te están pidiendo ya los puertos de conexión a través del cual hubo este este intercambio de material de uso sexual infantil.

En los Estados Unidos se utilizan las IPV6 y aquí también ya tenemos algunos proveedores que ya están utilizando las IPSV6, que básicamente son IP que están contratadas por una persona específica, un usuario final definido, lo cual a nosotros nos permite saber nombres y apellidos, quien es la persona que contrató ese servicio de internet en ese momento. Esto en los Estados Unidos nos permite a nosotros actuar de manera mucho más ágil en la prevención de estos delitos ya que al saber quién es la persona que está conectada y su ubicación, nosotros podemos actuar y rescatar en muchos casos para prevenir este delito antes de que sean consumados. En su gran mayoría, lo que nosotros trabajamos son casos ya reactivos porque muchas de las noticias criminales que recibimos ya se han efectuado los delitos.

Sin embargo, al tener la IPV6, nosotros podríamos prevenir para que estos delitos no lleguen a darse. Desafortunadamente el crimen siempre va un paso adelante, porque quiere ver la forma de ganar. Entonces no sé si realmente es efectiva la jurisprudencia ecuatoriana en la forma en la que si nosotros estamos un paso atrás todavía IPV4 cuando ya eventualmente la Corte Nacional desarrolle una jurisprudencia que contemple nuevos nuevas IP, va a ser realmente efectiva o

vamos a seguir un paso atrás, porque cuando ya la quizás la corte nacional desarrolle jurisprudencia como fuente del derecho para IPV6, probablemente ya habría otro tipo de tecnología.

En el momento actual incluso teniendo IPV6, con la ley de notificación creo que estaríamos incluso atados de manos, porque incluso sabiendo quién es el usuario final, si yo tengo que notificar a esta persona que está siendo investigada por un delito cibernético de material de abuso sexual infantil, no estamos velando por los derechos de quienes estamos tratando de proteger. Estamos de cierta manera favoreciendo al delincuente de este tipo de delitos, al notificarle que está siendo investigado y al ser un delito cibernético es muy volátil, pueden eliminar esa información de las bases de datos y pues nos quedamos, nos quedamos sin la evidencia que necesitaríamos para poder continuar con ese caso.

Entonces, más allá de incluso llegar a establecer un protocolo de internet IPV 6 se debería tratar el tema de la notificación no sólo para delitos de pornografía infantil que deberían primar ante cualquier otro delito, ya que atenta contra la población más vulnerable, sino que también reformar el tema de la notificación, reforzar el tema de la reserva de la investigación para este tipo de casos para poder tener un mayor éxito investigativo.

- **¿Qué herramientas legales considera que son necesarias para fortalecer la capacidad de investigación y persecución de este delito en Ecuador?**

  Bueno, para poner como ejemplo en los Estados Unidos, nosotros tenemos el código 18 hay. Específicamente que habla sobre la ley que obliga a todas las empresas que proporcionan Servicios de Comunicación, los ISP en el momento en que identifiquen que en sus servidores existe material de abuso sexual infantil o comunicación entre un adulto y un menor de edad, sea de manera sexual y

explícita, deben automáticamente reportar por ley, en este caso al Centro Nacional de Menores Desaparecidos y Explotados NCMEC. Estas empresas utilizan tecnología para poder realizar este tipo de denuncias, ya que existen sanciones muy altas por la omisión de este tipo de delitos al incumplir esta ley en la primera omisión, estamos hablando aproximadamente de 150000 dólares por omisión de delito y hasta 300000 dólares por omisiones de. Entonces, cuando hablamos de empresas de comunicación que se ven expuestas ante una legislación que les obliga a denunciar y el momento en que lo omiten o no identifican estos delitos están sujetos a sanciones económicas, se fuerzan generar o adoptar tecnología que les permita de manera más ágil ser parte de la solución de este tipo de delito.

Entonces por ahí empezaría en el tema de la ley que pueda ejercer este tipo de presión y por otro lado, es el tema del Convenio de Budapest, el momento en que el Ecuador ya se adhiere al convenio de Budapest. Podríamos nosotros de manera más ágil compartir información a nivel internacional, es decir, la evidencia de manera digital para poder procesar estos casos que son de índole transnacional.

Existen acuerdos que ya tenemos establecidos como agencia, específicamente con el Ministerio de Interior que nos permiten a nosotros poder proporcionar esta información de manera más ágil. Existe el proceso de asistencia penal internacional, pero todos conocemos lo demoroso de obtener esa información mediante este proceso, que no solamente implica preservar esa información en los servidores de la de la empresa que haya reportado a través de la cual se consumirá el delito sino, que es el tiempo que estamos exponiendo a los menores hasta que esta información llegue, están siendo vulnerados un día a la vez, un poco más. Entonces considero que obviamente tener una legislación que fortalezca el combate contra este delito, la adhesión al Convenio de Budapest y otros convenios

de colaboración internacional son claves para poder tener mayor efectividad en esta lucha.

- **¿Cómo evalúa usted la efectividad de las leyes actuales en la protección de los derechos de los niños y la prevención de la pornografía infantil?**

  Pues obviamente creo que estamos en el camino correcto, siempre hay algo que podamos mejorar. En ese sentido, háblese de la adhesión al Convenio de Budapest de la adopción de las IPSV 6 como norma para todo el Ecuador, háblese de convenios de intercambio de información, pero como digo siempre creo que vamos, mejorando, no creo que si hacemos un análisis de cómo empezamos hace dos 3 años, cuando empezamos a fortalecer este delito, estábamos en pañales y hoy por hoy, pues tenemos ya 3 unidades de la Policía Nacional especializadas.

  La Unidad de Ciberdelitos, la Unidad de Delitos Transnacionales a la cual nosotros auspiciamos, trabajamos también ahora con la Dirección Nacional de Niñez y familia y dentro de estas unidades tenemos personal altamente capacitado que día tras día analiza noticias criminales o cyber tips que provienen de varias empresas que proporcionan servicios de telefonía. Esto ha sido todo gracias a la colaboración internacional que hemos venido fortaleciendo en los últimos en los últimos años.

- **¿Cuáles son los principales desafíos técnicos y tecnológicos que enfrentan los operadores de justicia al investigar este tipo de delitos en el ciberespacio?**

  Bueno, principalmente creo que es el conocimiento. La tecnología avanza cada vez más rápido que en realidad se necesitan tanto investigadores, fiscales y jueces especializados en la materia para poder estar al día en lo que sucede, podemos hablar de criptomoneda, podemos hablar de delitos de material de abuso sexual infantil, inscripción en las plataformas, obviamente son temas bastante técnicos.

Qué es lo que nosotros veríamos como como un área en la cual podríamos mejorar, es obviamente adoptar las IPv6 a nivel nacional que nos permitirían tener este usuario final identificado de manera más ágil. Otra el tema de poder explotar los dispositivos tecnológicos in situ, si bien sabemos es importante, poder preservar la información que posiblemente esté alojada en las nubes de los dispositivos electrónicos, entonces tradicionalmente aquí se incautan los dispositivos, se los pone en modo avión fundas inhibidoras de señal para evitar cualquier manipulación.

Pero toda esta información es periciada días más tarde, entonces el momento en que nosotros conectamos un dispositivo de la nube, la cual posiblemente esté anclada, estamos perdiendo esa conexión a evidencia que posiblemente reposa en la nube y hoy por hoy, la mayor parte de los casos que vemos están siendo alojados en diferentes nubes de diferentes empresas que proporcionan estos servicios es por eso que creemos vital que dentro de las legislaciones dentro de los procesos se adopte para cualquier tipo de delito y específicamente en los delitos de material de abuso sexual infantil, la explotación in situ, para luego ser periciada días más tarde. Creo que esa sería algo clave que nos permitiría mejorar, el alcance investigativo porque esto nos permitirá identificar otras personas que sean parte de esta red hoy en día, la sextorsión que puede ser por temas financieros en la cual están extorsionando a menores o adolescentes por temas económicos o la extorsión por más material, por gente que busca obtener más material de uso sexual infantil. Entonces consideramos que para poder llegar a ese punto, obviamente las IPV6 serían claves y una vez que ejecutemos los temas operativos, el poder preservar y explotar esos dispositivos in situ de manera estandarizada en cualquiera de estos delitos creo que serían ideales.

La cuestión de explotar los dispositivos en el lugar, a nosotros nos ha servido mucho en algunos otros países que hemos trabajado, puesto que al momento que tenemos eso era una de las herramientas que utilizábamos para poder contrarrestar el problema de la versión cuatro, porque una vez que nosotros podíamos identificar a la persona, teníamos suficientes indicios para poder obtener una orden de allanamiento. Aunque no estamos 100% seguros, pero 90% de las veces hacemos porque cuadraba toda la información que teníamos de NCMEC. Lo miramos salir del café a la misma hora que estaba saliendo, entonces hacíamos la orden de allanamiento, explotábamos en el sitio y en Francia se arrestaba ahí mismo. Entonces esa era una de las herramientas que utilizamos porque tenía la posesión. Por ejemplo, Guatemala y Estados Unidos al momento que el investigador, el fiscal mira y tiene la imagen tiene la posesión, se le hace el cargo inicial de posesión. Obviamente después ya una vez que se explota y se examina todo eso y ya se le añaden los cargos que van a venir, distribución, producción, lo que sea que haya sido las imágenes que haya sido y al mismo tiempo nos ahorraría el problema.

No hay que olvidarnos que este es un delito que tiene víctimas detrás, muchas veces quienes desconocen la investigación pueden decir, bueno, están sí hay imágenes, pero las imágenes corresponden a niños, posiblemente del Asia o del África, y al no estar una niña o niño aquí en el Ecuador no hay delito y ese no es el caso, entonces hay que sensibilizar a los operadores de Justicia en este sentido. Poder explotar in situ para poder utilizar toda la tecnología que tenemos en identificar a víctimas. Muchas de las noticias criminales que nosotros recibimos corresponden a material de abuso sexual infantil conocido, es decir, material que ya ha sido identificado por un investigador en alguna otra parte del mundo que

corresponde a una menor de edad, niña ni adolescente, pero no nos tenemos que olvidar que mucho de este material está siendo producido aquí localmente en el Ecuador y para nosotros poder identificarlo y clasificarlo como tal y de esa manera desarticular a quienes estén en posición en posesión de ese material a nivel internacional tenemos que tener acceso a esa información.

- **¿Qué papel juega la cooperación internacional en la investigación y persecución de la pornografía infantil en Ecuador?**

  Bueno, hace 3 o 4 años que empezamos a impulsar este tipo de investigaciones aquí en el Ecuador en realidad no existía, no era muy conocido, no resonaba en el oído del ecuatoriano que esto podía ser una posibilidad. Sin embargo, a raíz de del esfuerzo que se ha venido haciendo con las noticias criminales o los ciber tips que recibimos desde el Centro Nacional de Menores Desaparecidos y Explotados a nivel global, creo que hemos venido identificando que esta es una problemática con un índice muy alto. Entonces la colaboración internacional en ese sentido ha sido clave en el combate contra este tipo de delitos. No solamente en la recepción de estas noticias criminales, porque si analizamos el fenómeno tradicionalmente hay un porcentaje muy bajo de víctimas o terceras personas que identifican que está pasando este tipo de delitos y lo denuncian, Policía, Fiscalía. En Estados Unidos, nuestro mayor aliado, son las empresas que proporcionan esta misma tecnología porque más del 90% de las denuncias o las noticias criminales que nosotros recibimos vienen automáticamente proporcionadas ya que estas empresas están adhiriéndose a la ley de los Estados Unidos. Esto explica también que ciertas empresas tienen sus servidores fuera de los Estados Unidos, porque de esa manera no responden legalmente.

Es otra cosa es el tema de las de los equipos de tarea en conjunto, pues nosotros en Estados Unidos trabajamos con otros entes federales para el combate de este delito, es decir, maximizamos el recurso no solamente del personal sino de la tecnología que está disponible para identificar, combatir y rescatar a víctimas de este delito.

- **¿Cuáles son las medidas más efectivas que podrían implementarse para mejorar la identificación y persecución de los responsables de este delito?**

  Bueno, en ese sentido, creo que reiteramos el uso o la adopción de las IPV 6 a nivel nacional. Creo que sería parte clave para iniciar una mejor investigación en este sentido, conjuntamente con una ley que nos permita de manera ágil facilitar tanto a la Policía y a la Fiscalía la preservación de esta evidencia con las explotaciones de dispositivos in situ. Entonces las IPSV6 son claves para poder iniciar, identificar no solamente al victimario, sino a las víctimas, recordemos que al ser delitos que están dándose a través de redes sociales o redes peer-to-peer (P2P) de par a par, por ejemplo, estamos hablando que un perpetrador, un ofensor sexual de menores, está en comunicación con una víctima directa a la cual está extorsionando o de la cual está obteniendo material de uso sexual infantil y de la misma manera en que nosotros podemos identificar a este sospechoso, teniendo la facilidad de las IPV6, nosotros tendríamos la facilidad de poder identificar y rescatar a estas víctimas en tiempo real.

- **¿Cuál es su opinión sobre el acceso a tecnología actualizado por parte de las autoridades encargadas de investigar la pornografía infantil?**

  Bueno, si bien es cierto, como habíamos mencionado, hemos dado pasos bastante grandes en los últimos 3, 4 años, uno de ellos ha sido el fortalecimiento de unidades especializadas de la Policía Nacional hoy por hoy tenemos ya 3 unidades

especializadas. Otro la creación de la unidad de ciberdelitos de la Fiscalía, que tiene como competencia también el combate contra delitos de material de abuso sexual infantil, creo que ese es un paso bastante grande que se ha dado a nivel de la Fiscalía. Sin embargo, quiero poner como ejemplo el sistema de protección infantil utilizado por nuestros colegas en Guatemala en conjunto con HSI se generó de igual manera que aquí la Fiscalía de ciberdelitos dentro de esta Fiscalía existe lo que nosotros denominaríamos un equipo multidisciplinario, en el cual está el fiscal, los peritos, los policías dentro de un mismo espacio., es como tradicionalmente se investigan estos delitos, pues obviamente estas unidades analizan cientos de noticias criminales y buscamos cuáles tienen mayor proyección operativa y judicial y pues en ese sentido se presenta un paquete investigativo ante Fiscalía, por medio de sorteo va ante cualquiera de las fiscalías y se empieza a impulsar la investigación de abajo hacia arriba. El sistema de protección infantil de Guatemala, lo que ofrece es que los mismos fiscales están receptando las noticias criminales y hacen un análisis previo de la de la información que están recibiendo.

Mediante oficio delegan a la unidad especializada, esto está ocurriendo, por favor, realice vigilancias, seguimientos y les dan todas las delegaciones requeridas para poder fortalecer estas investigaciones. De ahí es que las investigaciones fluyen muchísimo más ágilmente cuando vienen de arriba hacia abajo, es decir, desde el fiscal que está a cargo de la investigación, simplemente se delega a las unidades policiales para que hagan todo el tema de análisis en territorio o en campo.

- **¿Cómo podría mejorarse la coordinación entre las autoridades gubernamentales, las organizaciones no gubernamentales y el sector privado en la lucha contra este delito?**

Bueno, creo que ahí hablamos bastante, lo que es la colaboración como la creación o el fortalecimiento de comités de cibercrimen, involucrar a sociedad civil como por ejemplo Ministerio de Educación y algunos otros entes privados o gubernamentales al combate o la identificación, principalmente de este tipo de delitos. Muchas veces sentarnos en una mesa y tenemos a los entes de diferentes instancias. Policía, Fiscalía, sector privado, sociedad civil y básicamente servimos como mediadores y le decimos, miren, este es el problema, estamos todos aquí alrededor de la mesa, qué tenemos todos para aportar, creo que estas mesas de trabajo en las cuales se pueden identificar fortalezas de cada una de las instituciones públicas, privadas son claves para poder prevenir. Entonces, cuando hablamos de prevenir, hablamos no solamente de programas de prevención, sino que qué está a mi alcance dentro de mí, de mi sector, de mi área, como de competencia privado o público que pueda yo aportar para poder mitigar o identificar este tipo de delitos y pues el establecer a raíz de eso política pública como el código 18 que tenemos en los Estados Unidos.

- **¿Qué políticas públicas considera que son necesarias para prevenir la pornografía infantil y proteger a los niños en Ecuador?**

  Primero creo que se requiere una ley similar al código 18 de los Estados Unidos que se sume a este a este esfuerzo, al obligar a las empresas que están de primera mano en el alcance de la tecnología, tanto en niños, niñas y adolescentes a reportar o ser parte de este esfuerzo de prevención creo que es clave. Segundo está en el tema de las IPV6, que facilitarían el trabajo como investigadores, como entes de cumplimiento de la ley en identificar a los sospechosos y a las víctimas de estos delitos. El tema de la explotación de dispositivos in situ para preservar, identificar a víctimas que estén posiblemente siendo victimizadas aquí en el Ecuador.

Considero que la colaboración internacional es clave en ese sentido, porque existe mucha tecnología, mucha información como vivo ejemplo es el Centro Nacional de Menores Desaparecidos y Explotado NCMEC, sin él no estaríamos hoy hablando de este tipo de casos en el Ecuador y el éxito que se ha tenido.

Además, tenemos que hablar sobre la prevención, nosotros como agencia el 17 de abril de este de año vamos a lanzar la campaña iguardians, guardianes del internet, es una campaña que busca de manera efectiva prevenir que estos delitos sucedan entonces es mucho más fácil prevenir que una niña sea víctima de estos delitos que el investigarlo, dada la complejidad de las IPV4 y la complejidad de la legislación en diferentes países, pero también considero que hay que hablar, el tema de programas de prevención, a través del cual nosotros desde Estados Unidos estamos dándole una alerta temprana, en este caso al Ecuador de personas que posiblemente puedan poner en riesgo a la niñez y adolescencia. Hablamos también de posiblemente comparar un poquito la legislación en Estados Unidos cuando existe un delito contra menores de edad. Al igual que en Ecuador, existe la pena privativa de libertades, es decir, sirve en un tiempo de prisión. Nosotros verdad te podemos poner cargos uno por posesión, otro por distribución, otro por producción y agravantes, si es que tienes algún tipo de posición autoridad ante la ante la víctima o si hay algún tipo de discapacidad en la víctima, etcétera. Pues muchas de estas penas condenatorias tienen unas sanciones mucho más altas, incluso que el narcotráfico. En el Ecuador también tenemos algo similar, entonces comparamos ahí que estamos hablando un poquito, el mismo lenguaje, hablamos también de la reparación integral a la víctima. Muchas veces es algo que no se habla, no, a veces se deja muy de por un lado a la víctima, en Estados Unidos tenemos leyes que nos permiten utilizar lo que aquí se denomina la ley de

extinción de dominio, es decir, la persona que cometió estos delitos contra niño, niña o adolescente le podemos incautar sus que haya adquirido, ya sea por la por la comercialización de estos de estos delitos, que no olvidemos que hay nexos financieros en la investigación de estos delitos y esos son utilizados como parte de la reparación integral a la víctima. Aparte de eso, los pasaportes de los americanos que cometen delitos contra menores están marcados en la última página en la página 52 de anotaciones dice que el portador de este pasaporte o documento de viaje ha sido sentenciado como un ofensor sexual de menores bajo el código los Estados Unidos, entonces de esa manera, si es que viajan a países que no tienen una muy buena relación con Estados Unidos, pues al menos pueden ver esta está alerta temprana y decidir si es que van a dejar admitir a esa persona o no.

La restricción de poder vivir cerca de parques o escuelas creo que es clave porque conocemos ya de la experiencia que personas que llegan a delinquir en el tema de material de abuso sexual infantil son usualmente reincidentes. Entonces el mismo hecho que esté en proximidad cercana con menores en un parque, en una escuela, pone en riesgo a esa población de niños, niñas y adolescentes, y adicionalmente, pues obviamente nosotros notificamos a nivel internacional cuando están viajando.

Existe también un registro de ofensores sexuales registrados, es una página web pública en la cual uno puede ingresar el código postal, la dirección de en los Estados Unidos, donde uno reside o quiere comprar una casa y te van a salir, ahí todos los ofensores sexuales de menores registrados que viven en esa área. Entonces ahí trabajamos mucho, como como un comprador potencial de un de un domicilio en cualquier estado puede ingresar a esta página pública y evaluar si es

que existen muchos ofensores sexuales registrados en ese sector y posiblemente eso les ayude a tomar una mejor decisión y decidirse a otro barrio, a otro vecindario, a otra ciudad o estado donde exista menos incidencia de este tipo de personas. Entonces creo que por ahí se podrían considerar algunas áreas como para prevenir este tipo de delitos.

- **¿Cuáles son las lecciones aprendidas de casos anteriores de pornografía infantil en Ecuador y cómo podrían aplicarse para mejorar futuras investigaciones y procesos judiciales?**

  Cuando hablamos de casos anteriores, pues obviamente creo que siempre empezamos con mencionar que no son crímenes que no tienen víctimas. Creo que ese fue el reto inicial cuando empezamos a combatir estos delitos que por parte de entes de cumplimiento de la ley no había esa ese conocimiento, que decir, el niño o la niña era de otro país, pues no había delito aquí y se archivaba la causa porque no hay una víctima de por medio, la víctima no pone una denuncia, entonces no tiene el suficiente elemento para comprobarlo. Entonces creo que eso fueron algunos de los retos iniciales que empezamos a identificar que no había ese nivel de sensibilización.

  Hemos tenido varios casos desde que iniciamos este este tipo de lucha aquí en el Ecuador y pues creo que la falta de conocimiento, empezando con los mismos investigadores de Policía, Fiscalía y quienes ya ejecutan la ley en los tribunales era bastante.

  Otra área que teníamos que trabajar y pues desde entonces hemos venido realizando varias charlas, varios acercamientos, varias capacitaciones con estos diferentes entes para poder darles a conocer cuáles son las herramientas que están disponibles para combatir este delito, para prevenirlo y para identificar a víctimas

que están detrás de estos casos. La idea con este tipo de charlas, de conferencias de conversatorios o mesas de discos, es tratar de que todos los operadores de Justicia, empezando desde Policía, Fiscalía y los jueces podamos estar hablando el mismo lenguaje y entendamos un poquito la dinámica y la complejidad que existe en investigar este tipo de delitos.

También hablamos a nivel a nivel mundial hoy por hoy todavía muchas legislaciones se denomina pornografía infantil. Tal es el caso del Código Integral Penal donde se habla todavía de pornografía infantil, es algo que también ya ha ido evolucionando a nivel global. Hoy por hoy ya se denomina material de abuso sexual infantil y el porqué es muy simple, un niño o niña adolescente no tiene la capacidad para poder producir pornografía voluntariamente, es decir, el hecho de hablar de pornografía infantil, estamos diciendo que el niño o la niña tuvo la capacidad de hacer o realizar enviar este tipo de material y ese no es el caso, entonces uno de los primeros esfuerzos que estamos haciendo es cambiar esa connotación, esa esa idea de que es pornografía infantil, sino que ahora denominarlo como lo que es material de abuso sexual infantil donde víctimas están siendo explotadas, sea aquí en el Ecuador o en cualquier otra parte del mundo.

Cierre

Te agradezco por brindarme la entrevista, valoro mucho el tiempo que me ha concedido

Entrevista al Ing. Jorge C. Guerron Eras, experto en Ciberseguridad

Guía de Entrevista

Tema: El delito de pornografía infantil en el Ecuador dificultades investigativas

Objetivos: Determinar la relación del ciberespacio con el delito de pornografía infantil.

Evidenciar cómo inciden las direcciones IPV4 en la investigación del delito de pornografía infantil.

Persona Entrevistada: Jorge C. Guerron Eras

Persona que realiza la entrevista: Christian Alex Fierro Fierro

Fecha de entrevista: 29-06-2024

Presentación

Soy alumno de la "Maestría en Derecho Penal con Mención en Criminalidad Compleja" de la Universidad de las Américas UDLA. En este contexto como tema de investigación académica estoy investigando sobre "El delito de pornografía infantil en el Ecuador dificultades investigativas".

Solicitud de permiso

Quiero preguntarle antes de iniciar con la entrevista si usted está de acuerdo con que sea grabada, asegurándole que la información será confidencial y se utilizará únicamente con fines académicos

Desarrollo de la entrevista

Preguntas introductorias

Antes de comenzar con la entrevista cuénteme

- ¿**Cómo se llama?**
- Soy el Ing. Jorge C. Guerrón Eras, experto en Ciberseguridad
- **¿Cuál es su experiencia profesional en relación con delitos de pornografía infantil?**
- Bueno, yo trabaje en su momento como perito informático forense para la Función Judicial, calificado por medio del Consejo de la Judicatura y daba apoyo a los equipos de Criminalística y Policía Judicial en investigación de delitos contra niños, niñas y adolescentes.

- **¿Cuál es su opinión sobre la prevalencia y la gravedad del problema en el país?**
- Bueno de cierta forma en los delitos contra niños, niñas y adolescentes del caso de la pedofilia como tal o de la pornografía, frente a menores de edad, es bastante grade de cierta forma de lo que se denuncia a lo que se investiga termina siendo pequeño frente a la realidad frente a la realidad que yo he escuchado, porque cuando he tenido la oportunidad de cierta forma la investigación de este tipo de delitos uno se da cuenta que los atacantes se conocen entre ellos y tienen la capacidad de compartir su información, de compartirse mucha información como imágenes y videos de tipo explícito, contacto con otros atacante, existen en los procesos de investigación en lo que he estado involucrado grupos de whatsapp o grupos de redes sociales en los cuales justamente se da este tipo de incidentes no, entonces eso para poder tener presente.

Preguntas

- **¿Cuáles considera usted que son las principales dificultades que enfrenta la justicia ecuatoriana en la investigación del delito de pornografía infantil?**

  Yo creo que una de las principales dificultades de la justicia ecuatoriana ha sido justamente que hace unos 3 años no estaban bien tipificados estos tipos de delitos es más, esto recién comenzó a modificarse, a tratarse en relación con el Convenio de Budapest, mediante el cual se estuvo haciendo el proceso de adecuación normativa. Justamente una de las principales debilidades que enfrenta creo yo la falta de personal, el número de personal enfocado en el desarrollo de este tipo de investigaciones de delitos de pornografía infantil es uno de los principales problemas, fiscales especializados en este ámbito

también, o sea, cuando me refiero a personal, me refiero, por ejemplo, policial para este tipo de procesos de investigación y también jueces que entiendan sobre tecnología y sobre los elementos de convicción que presentan los señores investigadores y fiscales para la persecución y para que se pueda terminar juzgando sobre los indicios que se presentan en los casos de delitos de pornografía infantil.

- **¿Qué herramientas legales considera que son necesarias para fortalecer la capacidad de investigación y persecución de este delito en Ecuador?**

  Bueno, una de las herramientas que en este momento ya se está comenzando a utilizar a pesar de que no totalmente está desarrollada, es el Convenio de Budapest, creo que el apoyo que se ha dado jurídicamente, técnicamente y en materia de cooperación en la investigación de los delitos que se desarrollan por medio del internet y que tiene como objetivo la pornografía infantil ha sido muy importante en este último tiempo desde que ya se comenzaba con el proceso de firma del Convenio Europeo. La verdad que se ha visto mucho más efectivo el proceso de investigación de este tipo de delitos y se conoce por las noticias y se conoce por las comunicaciones que emite la Fiscalía General del Ecuador, que se está haciendo un ámbito, un trabajo mucho más fuerte en ese sentido.

- **¿Cómo evalúa usted la efectividad de las leyes actuales en la protección de los derechos de los niños y la prevención de la pornografía infantil?**

  Respecto a los derechos de los niños, aún creo que con los esfuerzos que se hacen del Estado no son suficientes, no van a ser suficientes en varios ámbitos y eso es uno de los elementos que ciertos problemas duelen a las personas que nos ha tocado estar atrás de los procesos de investigación, creo que no

solamente tiene que ver con un tema de ley, sino que sigue siendo bastante importante el tema de la cultura de que las familias, los padres, de las personas que se encuentran a su alrededor, de las víctimas de pornografía infantil tengan los canales de denuncia habilitados, creo que aún temas como la vergüenza de las familias, el hecho de que sean parte de las noticias o parte de las estadísticas, limita mucho el accionar investigativo y la persecución del delito, entonces, eso va a ser muy complicado de seguirlo desarrollando, pero creo que puede ir cambiado poco a poco.

- **¿Cuáles son los principales desafíos técnicos y tecnológicos que enfrentan los operadores de justicia al investigar este tipo de delitos en el ciberespacio?**

  Los principales desafíos, creo que son justamente el ámbito de poder compartir la información, nuestros operadores en ese ámbito investigativo, la verdad es que se hace muy difícil muchas de las veces en hacer una investigación sin las herramientas adecuadas, hacer la investigación sin licenciamiento, a veces hay dispositivos móviles y medios de almacenamiento masivo, discos duros, computadores, laptops, tablets con las cuales hay una posible información de evidencia que puede servir para los casos y si no se tiene las herramientas adecuadas, eso dificulta el proceso. Además, como todo corre en base a tiempos y no se tiene el número de personas de manera adecuada, eso dificulta también que los operadores de justicia puedan tener los elementos de convicción para la investigación de este tipo de delitos.

Entonces yo creo que justamente la falta de la herramienta, la falta de conocimiento técnico, la alta rotación que se genera, por ejemplo, inclusive en fiscalías o en la misma Policía Nacional, en los cuerpos especializados de la

policía, como son la Policía Judicial, Criminalística, va a seguir siendo un problema porque principalmente en estos cuerpos se les da capacitación ellos acceden a ciertas herramientas y los conocen de ciertas actividades. Sin embargo, el hecho de que cuando se les da el pase básicamente se pierde toda esa capacidad que se estaba generando. Entonces considero que son los principales problemas a nivel técnico, por la pérdida de conocimiento y a nivel de herramientas, porque el pago de licencias y el software muchas veces limita el accionar investigativo.

- **¿Qué papel juega la cooperación internacional en la investigación y persecución de la pornografía infantil en Ecuador?**

Es un papel muy importante, el papel es muy importante, justamente hace unos años yo les comentaba en un foro que tuvimos de investigación, por ejemplo, se identificó en que había comunicación de ciertos delitos de pornografía infantil y presentó que había chats de grupos con personas en México, en Chile, en Colombia, y pues en ese momento la cooperación no estaba tan eficaz como ahora, porque creo que sí hay oportunidades de seguir generando cooperación. Sin embargo, por ejemplo, las plataformas de redes sociales, grupos de whatsapp están allí y la oportunidad de que se genere investigaciones conjuntas de cooperación entre países, entre estructuras de investigación siempre va a ser muy importante eso, tanto para que nosotros podamos descubrir aquellos delitos en los cuales no se ha hecho una denuncia formal por parte de las víctimas, como cuando existen víctimas del país nuestro es de doble sentido, nosotros también debemos apoyar en esa cooperación, nosotros podemos apoyar en una investigación de este tipo de delitos y viceversa, cuando nosotros necesitamos y generamos una alerta para que esto se persigan otros países, también debería darse entonces esta cooperación que

es de doble vía y aunque ahora es más eficaz que hace cinco o seis años, aún hace falta algunas actividades por hacer.

- **¿Cuáles son las medidas más efectivas que podrían implementarse para mejorar la identificación y persecución de los responsables de este delito?**

Yo creo que justamente una de las medidas es la capacidad de que nuestras fuerzas del orden, de los cuerpos de investigación de este tipo de delitos, también de la Fiscalía que puedan ser de manera más rápida hacía, por ejemplo, las redes sociales hay muchísima información que se vaya, por ejemplo, a través de TikTok a través de Facebook a través de Twitter, inclusive el hecho de poder contar rápido con esta información va a ser muy importante, lo mismo que sucede, por ejemplo, con la tecnología que nosotros utilizamos, nosotros seguimos utilizando tecnologías que en algunas ocasiones genera dificultad. Las dificultades técnicas siempre se van a presentar, sin embargo la oportunidad de poder especificar de llegar a ciertos grupos va a ser siempre mucho mejor.

- **¿Cuál es su opinión sobre el acceso a tecnología actualizada por parte de las autoridades encargadas de investigar la pornografía infantil?**

Yo creo que ese sería un factor de cambio, justamente el hecho de que las personas puedan no solamente utilizar la tecnología, sino que nuestros grupos de investigación puedan materializar de manera efectiva esos eventos que suceden en el ciberespacio, para que pueda investigarse de mejor forma el tema de ciberdelitos. Justamente recordemos que una de las premisas del uso del ciberespacio para el cometimiento del delito es que se puede ocultar muchas de las veces este tipo de acciones que abarata este tipo de situaciones que permite ocultar, generar perfiles falsos.

Entonces, al ser el ciberespacio tan complejo, también genera esa complejidad y más que nada, las investigaciones se van realizando en función de las debilidades que los atacantes. Los delincuentes se siguen especializando, los delincuentes siguen aprendiendo técnicas y eso va a seguir dificultando el escenario de nuestros cuerpos de investigación.

- **¿Qué políticas públicas considera que son necesarias para prevenir la pornografía infantil y proteger a los niños en Ecuador?**

Yo creo que una política de educación, una política pública de educación que sea más efectiva va a ser muy necesaria. Una política pública de cooperación entre las instituciones que llevan a cabo estos procesos va a ser siempre muy importante de las instituciones que posiblemente trataron esas conexiones de esos datos también va a ser muy relevante. Entonces yo creo definitivamente en la cooperación política, y de educación, de ser responsables con los canales de denuncia con el manejo y la protección de las víctimas siempre va a ser muy importante para poder entender cómo llegaron hacia ellos y cómo se generó esos procesos va a ser un diferenciador para nuestro país.

- **¿Cuáles son las lecciones aprendidas de casos anteriores de pornografía infantil en Ecuador y cómo podrían aplicarse para mejorar futuras investigaciones y procesos judiciales?**

Justamente el accionar que nosotros podríamos generar viene dado y lo que se termina aprendiendo es sobre cómo se cometió el delito, qué hicieron las personas, cómo llegaron a las víctimas, cuáles fueron los mecanismos que se realizaron, generar un perfilamiento de por qué se hizo y cómo se llegó a esos eventos va a ser siempre muy importante aprender de lo que sucedido a documentar, ¿Cómo se realizó el proceso de investigación? También va a ser muy importante. Entonces,

dentro de las lecciones aprendidas, siempre que nosotros tengamos bien documentado que se tenga bien investigado, cuáles fueron inclusive las debilidades, las limitaciones para poder realizar los procesos de investigación va a seguir ayudando a que no se cometan los mismos errores y a que las personas sepan a quién, cómo dirigirse, cómo solicitar los pedidos de información e inclusive entonces esas lecciones aprendidas creo que son las más importantes.

- **¿Las direcciones IVP V4 ayudan en la investigación de pornografía infantil?**

No, en el tema de direccionamiento ni las direcciones IP versión cuatro ni las direcciones IP versión seis, van a ayudar o van a ser un factor influyente, si bien existen tecnología que se puede generar un mapeo, también existe el hecho que se puede genera el ocultamiento de direcciones IP, existe la oportunidad de que se pueda genera una falsificación, recordemos que tanto un celular, una computadora se comparten direcciones IP públicas en muchos ámbitos cuando se conectan las atacantes también pueden ir ocultando estos rastros de estas pistas de los ojos del investigador. Entonces, muchos de estos tipos de delitos los puede llegar a determinar por el tema de oportunidad, oportunidad de haber accedido a los dispositivos móviles que trataron a esa información, oportunidad de acceder a las cuentas que utilizaron, por ejemplo, en redes sociales para contacto de víctimas, entonces yo creo que está más enfocado en ese ámbito.

Las direcciones IP como tal, si bien son vinculantes para ver desde dónde se generaron en algunos casos las conexiones, lo más importante es el uso y dónde se contuvo ese material, cómo se estaba trabajando con ese material, yo creo que esa definitivamente también va a ayudar mucho a los operadores de justicia en esa parte. A nivel técnico puede hacer muchas cosas para poder ser un fantasma en la

red. Entonces un diferenciador, por decirlo de cierta forma, un atacante que está muy especializado, que por lo menos en nuestro país siguen cometiendo errores en ese ámbito, puede ser un punto de apoyo. Sin embargo, esto va a seguir evolucionando y ese no debería ser únicamente una de las premisas sobre las cuales se trabaje.

- **¿Cuál es su opinión sobre la pornografía infantil en la dark web?**

Justamente ese es uno de los elementos más complicados de análisis de la red oscura y de la red profunda porque recordemos que aquí existen sitios que van a seguir existiendo, sitios en los que se va a vender mucho de este tipo de material e inclusive, se vende víctimas dentro de este tipo de redes y el hecho de que nosotros no podamos ingresar que sean tan cambiantes las tiendas, que sean tan cambiantes los enlaces que no esté indexado nada de ese tipo de sitios va a seguir complicando. Justamente la evolución de la tecnología va a seguir complicando y el hecho de que tenga mecanismos de libertad a través de las redes también hace que los atacantes utilicen eso para el cometimiento de delitos.

- **¿El agente encubierto informático como una herramienta eficaz para la investigación de la pornografía infantil?**

Creo que es muy importante que como ciberagentes o como un agente encubierto dentro del ciberespacio, pueda tener la oportunidad de hacer los procesos de investigación, va a ser muy eficaz que se generen perfiles que utilice información falsa, también para poder llegar, para poder seguir para poder ser parte de estos grupos de trabajo de los delincuentes, que termina llevándole no únicamente a una idea de que se hace en el ciberespacio, sino que generen un contacto físico sobre los atacantes.

Entonces esos ciberagentes de cierta forma están comenzando a desarrollar sus actividades, siempre el objetivo final va a ser el poder llegar de manera física hacia estos delincuentes y eso es necesario que se proteja, es necesario que se indique cómo se hicieron, qué mecanismos se trabajaron y cómo se estuvo desarrollando esas oportunidades. Para los procesos de investigación y para poder determinar a los culpables de posibles delitos.

Cierre

Te agradezco por brindarme la entrevista, valoro mucho el tiempo que me ha concedido

Entrevista con EcuCERT (Ecuador Computer Security Incident Response Team)

Guía de Entrevista

Tema: El delito de pornografía infantil en el Ecuador dificultades investigativas

Objetivos: Recabar información sobre el rol de EcuCERT en la detección y respuesta a incidentes relacionados con pornografía infantil en línea.

Persona Entrevistada: José María Gómez de la Torre

Fecha de entrevista: 27-06-2024

Presentación

Soy alumno de la "Maestría en Derecho Penal con Mención en Criminalidad Compleja" de la Universidad de las Américas UDLA. En este contexto como tema de investigación académica estoy investigando sobre "El delito de pornografía infantil en el Ecuador dificultades investigativas".

Solicitud de permiso

Quiero preguntarle antes de iniciar con la entrevista si usted está de acuerdo con que sea grabada, asegurándole que la información será confidencial y se utilizará únicamente con fines académicos.

Desarrollo de la entrevista

Preguntas introductorias

Antes de comenzar con la entrevista cuénteme

- **¿Cómo se llama?**
- Soy el Ing. José María Gómez de la Torre, experto en Ciberseguridad
- **Preguntas:**
- **¿Cuál es el papel de EcuCERT en la lucha contra la pornografía infantil en línea en Ecuador?**

  Ya lastimosamente el EcuCERT no tiene una atribución específica para una actividad digamos de esta naturaleza. Sin embargo, un centro de respuesta de incidentes nunca debe dejar una denuncia de algún incidente informático sin atender pero sí no tiene la atribución, lo que debe buscar es el organismo competente dentro de la red digamos nacional de confianza o internacional incluso, entonces si llega un tema que no está en nuestro alcance, pero es un vecino país, se contacta al centro de respuesta de ese país nacional, se va siempre jerárquicamente con el nacional y se pide se atienda el tema, sea cualquier tema de incidentes, incluido el tema de pornografía infantil, que se considera también tecnológicamente como un tema de incidente informático por el tema del contenido, principalmente no es cierto que puede estar con tecnología adecuada, no porque los recursos tecnológicos pueden ser de punta, pueden ser avanzados, fuente de inteligencia artificial y todo, pero el contenido es nocivo y obviamente está penado en la mayoría de los países, entonces lo que se hace es buscar al par de ese país para que tome decisiones inmediatas, sea que desde ese país venga la

agresión. O sea que más bien desde nuestro país se está produciendo la agresión hacia el país amigo y se contacta al CECIR nacional de ese país.

Si el tema es a nivel, en cambio, de tratar de identificar dentro de nuestro país, la fuente o que se inicie una investigación, el responsable, digamos, de la investigación, en este caso es la Fiscalía, porque es un delito y normalmente cuando en un caso de este de este tipo puede ser de un fraude, puede ser de un acoso y puede ser un tema de pornografía, algo de algo ilícito, que tenga que ver con tecnología pero ha llegado a ser notificado como un incidente al EcuCERT, pues se interactúa inmediatamente con la Fiscalía o la Policía, no dependiendo a veces de la afinidad de la cercanía. No es una denuncia formal, pero sí se da paso para que se pueda proceder a una investigación formal y obviamente nosotros ya quedamos más bien a nivel de un experto técnico que en su momento incluso puede ser nombrado como un perito también técnico y apoyar en la investigación, pero no se puede tomar la posta, digamos, sino más bien entregarla a la autoridad competente para investigarla.

- **¿Cómo ha evolucionado la amenaza de la pornografía infantil en el ciberespacio ecuatoriano en los últimos años?**

  Si, bueno este a la final todos los ataques que se dan en el ciberespacio tienen una finalidad de lucro malsano como toda la delincuencia en cualquiera de sus formas, y puede ser robar señal, puede ser el robar directamente fondos a una institución o a los contribuyentes de una institución como por ejemplo un banco a través de ataques de phishing o robar directamente a una organización a través de un ataque de ransomware o este abusar y no respetar copyright o derechos de autor o temas ya de contenido como la pornografía infantil, que financian estas campañas, estos grupos y no es que estos grupos no solo se dedican a dañar algo en específico,

sino donde hay plata van donde tienen facilidades ellos, ellos van entonces muchas veces actividades como un ataque de fuerza bruta, un una organización como un ataque de acción de servicio, un ataque de ransomware, este también puede estar ligado a un tema de pornografía infantil. Y obviamente este genera bastante, bastante preocupación. ¿No es cierto? Dentro de la investigación y como mencionaba en el primer se busca rápidamente al a la institución que pueda tener la atribución de apoyar con eso. Ahora dentro de las atribuciones que tiene el EcuCERT al ser parte de ARCOTEL, es poder apoyar también con las operadoras telefónicas.

Entonces en muchas ocasiones en temas de delitos se tuvieron varias reuniones con policía o Fiscalía para apoyar este dando fuerza a los pedidos de información para que la labor de investigación investigativa, sea más ágil o se logre llegar a dar. No obstante, ciertas limitaciones tecnológicas siempre son bastante complejas, y había necesidad también de hacer algunos cambios regulatorios que en su momento se fueron dando de a poco, pero que a mi criterio todavía falta mucho que hacer para que la Fiscalía, la policía en delitos de contenido puedan hacer un buen trabajo. Ahí hay deudas a nivel del COIP a nivel jurídico para que puedan hacer una buena investigación.

Pero también hay deudas a nivel de regulación y tecnología para que los pedidos de investigación sean más efectivos y sean automáticos que no necesitemos de un seguimiento exhaustivo en cada caso, porque son muchos casos, muchos fiscales a nivel a nivel nacional, muchos procesos de fraudes y de casos de delitos con contenido y de pornografía infantil también que debería ser algo que funcione automáticamente hacia las empresas de telecomunicaciones puede hablarse incluso de un portal donde los entes de investigación pudiesen rápidamente

recabar la IP o a través de la IP del time stamp, o sea del tiempo en el que y el ahora en el que se cometió el delito, obtener información valiosa para poder llegar a conclusiones importantes dentro de la investigación.

- **¿Qué dificultades técnicas enfrentan al rastrear actividades relacionadas con pornografía infantil en línea?**

  Las dificultades técnicas son demasiadas, por eso hablaba de la necesidad de hacer una estrategia y esa estrategia que tiene que dar una solución tecnológica, pueda incorporarse a la regulación y que sea de obligatoriedad de cumplimiento de las operadoras telefónicas. ¿Por qué? Porque obviamente hay temas que casi que impiden realizar una investigación, si el tema de la IPV4 con el dateo de IP pública e IP privada es un factor muy, muy complicado, el tema de proxys es muy complicado, el tema de VPNS también es muy complicado de solventar, y el tema de que no haya una homologación de otros delitos con otros países y ser parte de documentos o convenios importantes como Budapest, pues impiden que se pueda hacer una investigación interna o externa. Lo hemos vivido en muchos tipos de delitos incluido el de pornografía infantil, apoyado como digo bien al ente que tiene la atribución como la Fiscalía y la policía, finalmente se logró en algunos casos, sí llegaron un poquito más allá, pero este las obligatoriedades que se pueda tener sobre las tercos no son suficientes como para poder llegar a tener un nivel de automatización y agilidad en la atención de resultados en la investigación.

- **¿Cómo impacta el uso de tecnologías como CGNAT, VPNs y la dark web en sus capacidades de detección?**

  Totalmente, imagínate eso es justamente donde se escuda normalmente quien va a delinquir, normalmente busca alguna de estas estrategias para esconderse hoy por hoy, incluso mucho del ramsomware, mucho de los delitos que se cometen a

través de la tecnología. Además de buscar el tema la dark web y de buscar extenderse a través de una VPN también lo hacen ahora a través de redes sociales, entonces, grupos de telegram, grupos de Instagram o de X son utilizados justamente para hacer transacciones y es muy usual que X sea utilizada y se haya incluso visto como una antesala a temas como Only Fans, lastimosamente son redes muy volátiles, grupos muy volátiles que son muy difíciles de ubicar y que digamos la transnacionalidad que tenemos de estas empresas privadas extranjeras hace que sea muy difícil y también lenta la investigación, al menos en el tiempo que yo estuve y traté de apoyar en los casos de investigación a la Fiscalía y la policía.

- **¿Cómo coordina ECUCERT con la Fiscalía y la Policía Nacional en casos de pornografía infantil?**

  Sí, normalmente, se actúa desde la parte de cooperación tecnológica dando cursos técnicos que permitan entender posibles soluciones o caminos más rápidos para tener resultados, reuniones donde hemos tenido, reunidos tripartitas digamos entre la autoridad, no cierto Fiscalía y Policía, empresas de telecomunicaciones o de Internet y el EcuCERT para facilitar este intercambio de información y finalmente muchas veces ha habido una cooperación técnica y en algunos casos, no recuerdo si específicamente en pornografía, pero si en muchos delitos de contenido, apoyar también como peritos técnicos en algún proceso con algún profesional de la EcuCERT o de ARCOTEL.

- **¿Existe colaboración con organizaciones internacionales como NCMEC? ¿Cómo funciona?**

  No, no recuerdo el nombre ahorita, pero había una empresa similar NCGME no recuerdo ahora el nombre ellos permitían o iban a apoyar cuando tuvieran una

hotline, incluso con recursos económicos, servidores, programas y todo, sin embargo, en su momento no se logró concretar como país una propuesta que sea viable sobre todo porque no había un actor que quisiese o que tuviere la atribución para adoptar, dar y garantizar que las acciones se concreten con estos organismos pudieran llegar a ser cristalizadas en la lucha frontal en delitos como la pornografía infantil o el acoso o cualquier tema, entonces lastimosamente si hubo coordinación con alguna empresa privada pero no recuerdo el nombre como UNICEF también había fondos, mucho apoyo pero a la final el tema de atribuciones en el país no estaba bien definido que a la final no hubo como dar viabilidad a ningún proyecto en ese sentido.

- **¿Cuenta ECUCERT con las herramientas tecnológicas necesarias para detectar y rastrear material de abuso sexual infantil en línea?**

  No, lastimosamente, no nunca se llegó a tener esas capacidades, tuvimos el ofrecimiento de tener un punto de o un servidor, mejor dicho, un servidor con esa capacidad, pero a la final se retiró el apoyo por parte de la Cooperación Internacional, en virtud de que no había una posición nacional que permitiera justamente aprovechar la donación de este tipo de equipamiento o de capacidades o de tecnología para poder rastrearse este tipo de material.

- **¿Qué tipo de capacitación especializada recibe el personal de ECUCERT en esta área?**

  En esta área, no, nunca se llevó a recibir tampoco ningún tipo de capacitación, más bien en virtud de la problemática de incidentes correlacionados que afectaban a los niños y adolescentes, pues se hicieron algunas investigaciones, algunas participaciones en charlas en algunas institución como es el Consejo de Niñez y Adolescencia, como el Ministerio de Educación y a la ciudadanía en general, a fin

de más bien tener una labor más bien preventiva, desde el cyberbullying hasta el tema de pornografía infantil, dando más bien consejos a la ciudadanía, a las instituciones en virtud de las problemáticas que veíamos desde los incidentes que eran denunciados al EcuCERT y finalmente era concientizar en varias ocasiones algunos segmentos de la sociedad, algunos colegios, realmente también barrimos varios colegios a nivel nacional indicando el cuidado que deben tener frente a las amenazas al ciberespacio y entre éstas el tema de la pornografía, caer en redes de pornografía infantil, el modos operandi era bastante conocido por nosotros en virtud de los casos que íbamos estudiando y esas eran las recomendaciones que se les daba en los colegios para que no llegasen a sufrir, el estar involucrados en la red de este tipo de mafias.

- **¿Podría compartir estadísticas o datos recientes sobre incidentes relacionados con la explotación y abuso sexual infantil en línea?**

  No, eso si no dispondría porque primero ya deje el EcuCERT hace varios años atrás y de hecho ahorita en el EcuCERT tampoco se manejan estadísticas en ese sentido, lastimosamente de la experiencia topada con las familias con las charlas que hemos dado en colegios sabemos que no denuncian, o sea que se lo guardan y por eso era la intención de que cuando tuviese una hotline para que haya una primera etapa de mayor cercanía a la ciudadanía con tipos psicológicos que puedan entender un poco, guiar un poco a estas personas a través de la hotline, pero que en su momento, ya con una mayor confianza y mayor certeza del apoyo que se les da por también iniciar las acciones de investigación, pero esto no se ha logrado concretar y es una deuda totalmente como país que tenemos con la ciudadanía, hablo desde todos los sectores, desde nuestro gobierno desde el Consejo de los Niños y Adolescentes, desde la Fiscalía, desde el INTEL, desde la

ARCOTEL, desde entidades, incluso internacionales como UNICEF, de esta deuda, digamos, como país desde las instituciones pública para algún rato se logre cristalizar.

- **¿Cómo se gestionan estos casos desde la perspectiva de ECUCERT?**

  Como bien decía, es como en cualquier tema que sea un delito y más aún, si no son tecnológicos, sino un delito de contenido se notifica a la Fiscalía, normalmente no como una denuncia porque no tenemos digamos un conocimiento que recuerdo, al menos exhaustivos o claros del problema, ni siquiera la certeza de que sea exactamente en qué tipo de delitos que se están cometiendo pero si un traslado de la inquietud o de la IP que podría estar haciendo eso o del dominio desde el cual se podría estar produciendo esto, o de las redes de la cual se está produciendo para que sea la autoridad, en este caso con las atribuciones adecuadas que pueda gestionar la investigación.

- **Desde su perspectiva, ¿qué mejoras en la legislación o en las capacidades tecnológicas serían necesarias para combatir más eficazmente este delito?**

  Claro, la capacidad investigativa tecnológica deberían poder involucrar de una manera más directa a las empresas de telecomunicaciones, si bien es cierto, digamos es un campo que normalmente no desharían entrar, de la experiencia que yo recuerdo, sin embargo, es muy necesario dar este voto a favor del país, en favor de la ciudadanía y hacer ese esfuerzo de apoyar frontalmente las investigaciones, hay muchas formas actualmente de poder apoyar incluso en casos difíciles como en VPNs o en la figura del mapeo que se hace desde una IP pública a una IP privada.

  Sin embargo, son temas que involucran cierto nivel de conocimientos tecnológicos y realmente un apoyo decidido para la investigación, temas que en

la regulación no se encuentra actualmente y por ende si debieran instrumentarse para lograr tener una mejor trazabilidad hacía la fuente del problema que se haya podido identificar. Y jurídicamente el COIP, hay algunos estudios que están en la mesa, recuerdo algunos que participe con varias instituciones que ya están para la aprobación de la asamblea, pero entiendo que hasta el momento no han sido aprobados, incluso no somos parte del Convenio de Budapest y tenemos esta dificultad digamos de interactuar con otras autoridades policiales o de investigación en otros países.

- **¿Qué tendencias futuras prevén en relación a la pornografía infantil en línea en Ecuador?**

  La tendencia es, yo pienso a seguir vigente, en virtud de que es un delito de cuello blanco que es bien difícil identificar actualmente, mientras no se hagan estas mejoras tecnológicas y legales en el país, pues Ecuador seguirá siendo un territorio que permita alojar a bandas criminales que abusan de nuestros niños y adolescentes, y generan este tipo de material, que primero venden al mundo directamente como tal y segundo, no sólo el material, sino los niños o adolescentes que figuran ese material son incluso etiquetados y luego también pueden ser consumidos en turismo sexual en el país o incluso trata de menores.

  Entonces el problema es más grave, a veces de sólo tener un video que de por sí ya es muy malo, sino que puede ser mucho peor para esos niños, sobre todo cuando lograban vulnerar también a los papás o a los que muchas veces son niños huérfanos, niños que viven con los abuelos o con familias que no tienen recursos y también con algo social se les puede convencer y ahí vienen temas de trata, pero nace de un video donde algo en un país del primer mundo, pues elige a ese niño, se los llevan después para consumo sexual o al revés vienen al país y son utilizados

digamos como en un video o en la forma infantil como una especie de menú para seleccionar este cuál o qué es lo que va a consumir entonces el tema debe ser atacado desde la pérdida infantil para reducir muchos otros de los delitos que pasan.

Cierre

Muy bien, te agradezco mucho por brindarme está esta entrevista. Valoro mucho tu tiempo que me has concedido. Muchas gracias.