



Artículo original

Falta de identificación del autor en causas generadas por el Sistema Cybertipline¹ Lack of perpetrator's identification in cases generated by the CyberTipline system Káusakuéra osêva Sistema Cybertipline rupive hasy ojejuhu haguã ijapoharépe.

Tatiana Cesario *

<https://orcid.org/0000-0001-5289-872X>

Ministerio Público. Instituto de Altos Estudios Estratégicos. Asunción, Paraguay*

Resumen

En el año 2013, el Ministerio Público del Paraguay suscribió un convenio con la entidad no gubernamental denominada Centro Nacional para Niños Desaparecidos y Explotados de Estados Unidos en adelante NCMEC. El acuerdo consiste en la cooperación entre ambas instituciones, por parte del NCMEC, el acceso a una VPN a su Sistema *Cybertipline* que resguarda reportes de casos de pornografía relativa a niños, niñas y adolescentes, denunciados por la proveedora de servicios electrónicos, en los que el supuesto autor haya utilizado una dirección de IP, cuya geolocalización corresponda a una empresa proveedora de internet, que fije residencia en el país. En tal sentido, se de apertura a una investigación de cada caso por parte del órgano investigador. Con ese fin, la presente investigación tiene como objetivo general identificar los obstáculos que existen en la investigación de los casos de pornografía infantil denunciados a través del mencionado sistema. Con ese fin, se analizan las causas que ingresan a través del Sistema *Cybertipline*, entre los años 2014, 2015 y el

Recibido: 17.09.2021

Aceptado: 29.10.2021

¹Este artículo es un resumen adecuado a partir de la tesis presentada para la obtención del título de Especialista en Ciberseguridad y Ciberdefensa Estratégica del Instituto de Altos Estudios Estratégicos en el año 2020.

*Secretaría fiscal de la unidad n°. 1, Especializada en Delitos Informáticos, del Ministerio Público. Asunción, Paraguay. Email: tcesario@ministeriopublico.gov.py

Abogada egresada de la Universidad Católica de Asunción, Especialista en docencia superior por la Universidad Católica de Asunción, Egresada de la Escuela Judicial Fuero Penal, Especialista en Ciberseguridad y Ciberdefensa Estratégica por el Instituto de Altos Estudios Estratégicos, Masterando en Ciencias Jurídica en la Universidad Católica de Asunción.

ISSN 2415-5063 versión impresa

ISSN 2415-5071 versión en línea

<https://ojs.ministeriopublico.gov.py>

Contacto: dip.informaciones@ministeriopublico.gov.py



Artículo de acceso abierto. Licencia Creative Commons 4.0.



2016, para determinar las dificultades e identificar a los autores de las causas denunciadas en los que no se puede determinar al autor. Es importante resaltar el esfuerzo y la voluntad puesta por el Ministerio Público para investigar y combatir esta criminalidad, sin embargo, existe una brecha amplia entre los casos denunciados y los casos con condena en razón a las dificultades que se presentan al investigar un hecho punible ocurrido en el ciberespacio.

Palabras claves: NCMEC, Cybertipline, pornografía infantil, dificultades

Abstract

In 2013, the Public Ministry of Paraguay signed an agreement with the non-governmental entity with the National Center for Missing and Exploited Children of the United States, from now on NCMEC. The agreement consists of the cooperation between both institutions, by NCMEC giving access to a VPN to its Cybertipline system that has reports of cases of pornography related to children and adolescents reported by the electronic service provider in which the alleged perpetrator has used an IP address whose geolocation corresponds to an internet provider company that establishes residence in our country and the investigation of each case by the Paraguayan prosecutor's office. The general objective of this research work is to establish the obstacles that exist in the investigation of cases of child pornography reported through the Cybertipline system. The specific objectives are; determine the average number of causes that enter through the Cybertipline system per year between the years 2014, 2015 and 2016, fix the difficulties to identify the perpetrators of the causes reported in the mentioned period of time and identify measures assigned or adopted in the Cases of child pornography reported through the Cybertipline system in which the perpetrator cannot be determined.

Keywords: NCMEC, Cybertipline, Child Pornography, Difficulties

Ñemombyky

Upe ary 2013, Tetãygua Motenondeha Paraguái pegua omopeteĩ iñe'ẽ ha oñembokuatiaconvenio rupive peteĩ entidad hérava Centro Nacional para Niños Desaparecidos y Explotados de Estados Unidos ingles ñe'ẽme NCMEC-ndi. Ko ñe'ẽme'ẽ ojapo hikuái oñomoirũ haguã mokõi temimoĩmby, Pe NCMEC ombokatuojeike haguã, VPN Sistema Cybertipline-pe upépe opytapa hína umi káso pornografía mitã'i, mitãkuña'i ha mitãrusúrerehegua, oñedenuncia haguépe ojapova'ekue umi proveedora de servicios electrónicos, umi oje'éva mba'evai apohare oiporuhagueIP dirección, ha ojehekávo geolocalización rupive ojejuhu ha'eha empresa ome'éva internet, oñembohógavaParaguái. Upéicha rupi, oñemoñepyry peteĩinvestigaciónohapykuere rekáva peteĩteĩ umi káso, kóva opyta pe órgano ohapykuerereka va'erãme Upévagui, ko investigación rupive ojehechakase mba'emba'épa umi javorái ojokóva ani haguã oku'e umi investigación ohapykuere rekáva ko'ã kaso pornografía infantil rehegua oñedenunciava'ekue pe sistema ryepýpe oiko va'ekue 2014, 2015 ha 2016 pukukue, ojejuhu haguã mba'emba'épa ijetu'uvéva ojejuhu haguã mba'evai apohare oñedenunciava'ekuépe. Tekotevẽ avei ojehechakuaa hendápe porã Tetãygua Motenondeha oñeha'ãmbaite ohapykuerereka ha ohapejoko haguã ko crimen, upéicharõ jepe, heta gueteri ofalta ojoja haguã káso oñedenciáva guive oñeguahẽ haguã



condena-pe, ko'ã mba'e ijetu'úva rehe oñeñepysanga rupi ko'ã mba'evai apoha ciberspacio-pe.

Ñe'ẽ tee:NCMEC, Cybertipline, mitã ñembo'opíva, javorái.

Introducción

Antes de que la red de redes fuera un medio indispensable para el desenvolvimiento de la vida, el individuo con un patrón de conducta sexual enfocada en niños, niñas o adolescentes, centraba su atención hacia el menor, merodeando parques y escuelas hasta fijar una persona de su interés para luego obtener más información. Al respecto, el medio para concretar sus fantasías sexuales por lo general era el secuestro.

A la luz de esta problemática, en el año 1984, en la ciudad de Virginia de Estados Unidos de América, surge el Centro Nacional para Niños Perdidos y Explotados, en adelante NCMEC, una organización privada cuya finalidad es brindar servicios a familias y profesional es para la prevención de casos en donde un niño o niña se encuentre en una situación de peligro, sean secuestrados y/o sean explotados.

Con los adelantos del internet, la modalidad de comisión de estos hechos cambió. Los pedófilos –persona que siente atracción sexual hacia niños, niñas o adolescentes– se beneficiaron de la privacidad, anonimato y fuente ilimitada de menores en las redes sin supervisión, facilitando medios para satisfacer sus fantasías (Medaris M. y Girouard C. 2002).

Ahora bien, con la finalidad de cumplir su objetivo el NCMEC desarrolló el proyecto denominado *Cybertipline* – sistema de informes centralizado del país para la explotación infantil en línea–.

Desde el año 2008, las empresas proveedoras de servicios electrónicos –*Electronic Service Provider*, en adelante ESP– se ven constreñidas a proveer información como dirección de correo electrónico, dirección de Internet Protocolo, en adelante IP, la geolocalización de la empresa proveedora de internet, número de teléfono asociado a la cuenta de sujetos sospechosos de la reproducción, compartir o poseer pornografía infantil.

Con la aplicación del proyecto *Cybertipline* de NEMEC por los EEUU, varios reportes contemplaban direcciones de IP provenientes de países extranjeros, por lo que en un esfuerzo por no dejar los casos impunes empezó a firmar convenios con varios países, para remitir los casos en los que se estuvieran cometiendo el hecho con direcciones de IP internacionales.

En tal sentido, el Ministerio Público de la República del Paraguay, en el año 2013 firma el convenio con NEMEC para unir esfuerzos internacionales por acabar con el flagelo del abuso sexual en menores y la pornografía infantil.

A partir de la firma del mencionado convenio, los casos de pornografía relativa a niños, niñas y adolescentes aumentaron a una cantidad exorbitante. Los obstáculos en muchos casos significaron la falta de identificación del autor, por lo que el resultado de las investigaciones son infructuosos y no permiten el castigo previsto en las leyes penales.

Por tanto, esta investigación tiene objetivo establecer los obstáculos que existen en la investigación de los casos de pornografía infantil denunciados a través del Sistema *Cybertipline*.



Para ello, se determinará el promedio de causas que ingresan a través del Sistema *Cybertipline* por año en los años 2014 y el 2016, así como también expresar las dificultades para identificar a los autores de las causas denunciadas en este periodo. Igualmente, se indicará las medidas adoptadas en los casos de pornografía infantil reportados a través en los que no se puede determinar al autor.

El Ministerio Público de la República de Paraguay ha reunido esfuerzos para hacer frente a la lucha de la cibercriminalidad, en especial contra la pornografía infantil, sin embargo, existe una brecha bastante amplia entre los casos denunciados y los casos con condena en razón las dificultades que se presentan al investigar cuando éstas ocurren en el ciberespacio.

Marco Teórico

Función del Ministerio Público en el sistema de justicia paraguayo

En ese entendimiento, se presenta su rol de representante de la sociedad ante los órganos jurisdiccionales, para promover la acción penal pública en defensa de los derechos consagrados en la Constitución Nacional.

En el hecho punible de pornografía infantil, cuya prevalencia es el interés superior del menor y el bien jurídico protegido es su desarrollo integral, se encontró con varios obstáculos en la prosecución de la investigación de este tipo de hecho punible reportados a través del Sistema *Cybertipline* del NCMEC.

Pornografía relativa a niños, niñas y adolescentes

La pornografía relativa a niños, niñas y adolescentes se encuentra reglamentada por la Ley n.º 4439/11, que modifica y amplía varios artículos de la Ley n.º 1160/97 “Código Penal”. En esa línea, art. 140, de la Pornografía relativa a niños, niñas y adolescentes, establece:

1º El que:

1. produjere publicaciones, en el sentido del Artículo 14, inciso 3º, que representen actos sexuales con participación de personas menores de dieciocho años de edad o la exhibición de sus partes genitales;
2. organizará, financiara o promocionara espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años en la realización de actos sexuales, o;
3. distribuyera, importara, exportara, ofertara, canjeara, exhibiera, difundiera, promocionara o financiara la producción o reproducción de publicaciones en sentido del numeral 1, será castigado con pena privativa de libertad de hasta cinco años o multa.

2º El que reprodujera publicaciones según el numeral 1 del inciso 1º, será castigado con pena privativa de libertad de hasta tres años o multa.

3º La pena de los incisos anteriores podrá ser aumentada hasta diez años cuando:

1. las publicaciones y espectáculos en el sentido de los incisos 1º y 2º se refieran a menores de catorce años o se dé acceso a los menores de dicha edad a publicaciones y espectáculos, en sentido de los incisos citados;
2. el autor tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo;



3. el autor operara en connivencia con personas a quienes compete un deber de educación, guarda o tutela respecto del niño o adolescente;
 4. el autor hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie; o
 5. el autor actuara comercialmente o como miembro de una banda dedicada a la realización reiterada de los hechos punibles señalados.
- 4° El que obtuviera la posesión de publicaciones en el sentido de los incisos 1° y 3°, será castigado con pena privativa de libertad de hasta tres años o con multa.
- 5° Se aplicará, en lo pertinente, también lo dispuesto en los Artículos 57 y 94.

Centro Nacional para desaparecidos y niños explotados

El departamento de Justicia de los Estados Unidos de América provee de fondos al NCMEC, ya que sirve como un centro nacional de recursos de información relacionada a delitos contra los niños.

El centro también mantiene *Cyber Tipline* para recibir denuncias sobre hechos de pornografía de los ESP y miembros del público en general (*United States Government Accountability Office* 2011).

El personal del NCMEC revisa cada *Cyber Tip* –pista informada a la *Cyber Tipline*– y trabaja para encontrar una ubicación del incidente denunciado a fin de, ponerla a disposición de la agencia de fuerzas del orden correspondiente, para que se inicie una posible investigación.

Empresas proveedoras de internet

El internet proporciona un medio sin igual para el acceso irrestrictivo a la información, las empresas proveedoras de estos servicios denominada *Internet Service Provider*, en adelante ISP, entendida como la suministradora de servicio de acceso a internet al usuario (Sutter, 2005) ofrecen atractivos servicios para facilitar la comunicación e incluso llegan a reemplazar interacciones sociales.

El impacto de este medio ha sido determinante en la vida de cada uno de sus usuarios. Dentro de estos últimos se puede contar a un número importante de personas que no han cumplido la mayoría de edad –tanto por ley como por las regulaciones marcadas por cada una de las redes sociales o servicio a los que tuvo acceso por internet– y que se encuentran navegando las redes sin supervisión alguna.

Empresas de servicios electrónicos

ESP cuya tarea principal se enfoca en sistematizar datos complejos para su transporte en bits simples desde el extremo emisor del sistema, para transmitir estos bits y reconstituirlos en forma compleja en el extremo receptor, para proveer plataformas de correo electrónico, sitios de redes sociales e intranets corporativas (E. Braganza 2013).

Las denuncias de casos de pornografía relativa a niños, niñas y adolescentes realizados por empresas como Google, Facebook, Instagram, Twitter etc., con sede en Estados Unidos de



América, contemplan dentro de sus condiciones de uso que cualquier acto indebido será alertado a las autoridades correspondientes. Estas informaciones, son procesadas por la Coordinación de Apoyo Técnico de la Unidad Penal Especializada en Delitos Informáticos del Ministerio Público.

Dirección de Internet Protocolo

La IP interviene una vez que una parte emisora decide transmitir un flujo de datos, que se analiza en una serie de paquetes de datos más pequeños. Cada paquete contiene un encabezado, que es una etiqueta de identificación que contiene la dirección IP de envío y de destino que posibilita identificar a un usuario (E. Braganza 2013).

Dificultades para identificar a los autores en las causas denunciadas a través de Cybertipline

Bajo la autorización del Congreso de los Estados Unidos de América por Ley n.º 42 U.S.C. § 5773, NCMEC opera con *Cybertipline* y el programa de identificación de víctimas para proveer asistencia a las fuerzas del orden y otros en sus esfuerzos para identificar y rescatar a víctimas de pornografía infantil y explotación sexual infantil.

Así también, NCMEC trabaja con las proveedoras de servicios electrónicos, servicio de pago electrónico y otros con el fin para reducir la distribución de imágenes y videos de explotación sexual infantil en internet.

En ese contexto, es importante resaltar que no investiga ni puede verificar la veracidad de la información que recibe, su función es poner a disposición los reportes de aparente explotación sexual infantil a las fuerzas del orden, para su revisión y análisis correspondiente.

En el año 2013, el Ministerio Público de la República del Paraguay suscribió un convenio dicha organización, consiste en otorgar acceso a funcionarios suficientemente autorizados a una red privada virtual denominada *Virtual Private Network*, en adelante VPN, que alojan los reportes realizados por las empresas proveedoras de servicios electrónicos relacionados a incidentes que se enmarcarían dentro del tipo penal de pornografía infantil y cuya geolocalización se encuentre en el territorio de la República del Paraguay a fin de que, los incidentes sean investigados.

Las denuncias realizadas por medio de la mencionada cooperación por su significativo número debieron ser distribuidos entre las dos unidades penales especializadas en Delitos Informáticos, en adelante UEDI y las tres unidades especializadas en Trata de personas y explotación sexual en niños, niñas y adolescentes, en adelante UFETESI.

Los reportes pueden contener una variedad de información adicional, incluidos los datos recopilados de búsquedas en sitios web de código abierto disponible públicamente, esta información es denominada de fuente abierta y se discute actualmente sobre su validez en los procesos penales ya que no existe como figura procesal y su autenticación puede acarrear problemas de fiabilidad.

Esto último dada la facilidad de crear correos falsos y la falta de control al consignar datos personales en redes sociales, existen muchos casos de suplantación de identidad, figura que no se encuentra contemplada hasta la fecha por la legislación nacional.



A parte de la gran cantidad de reportes, cabe destacar que los informes se encontraban totalmente escritos en inglés, por lo que los técnicos no solamente debían imprimir el informe y guardarlo en formato magnético, sino que también traducirlo al español a fin de que los investigadores comprendan el contenido de los documentos.

La relación de tiempo entre la recepción de los reportes, el procesamiento y la remisión de a las unidades penales para su posterior investigación comprende un trabajo minucioso. Podría pasar seis meses hasta que una denuncia sea formalmente ingresada. Esta situación ocasiona que las empresas, que poseen datos de los números de teléfono asociados a las cuentas sospechadas de haber incurrido en el art.140 del Código Penal modificado por Ley n.º 4.439/11, por lo que ya no están obligados a la retención de datos.

Medidas adoptadas en los casos de pornografía relativa a niños, niñas y adolescentes en los que no se puede determinar al autor

El Código Procesal Penal paraguayo señala que, en el supuesto en que, tras haberse realizado con el auxilio de los organismos de investigación, las diligencias investigativas o bien, las pesquisas correspondientes para la individualización de los autores o partícipes del hecho reputado criminoso, no se haya podido individualizar, el Ministerio Público podrá disponer fundadamente, el archivo de las actuaciones.

Para llevar a cabo este procedimiento legal, la Ley n.º 1286/98 CPP faculta al Ministerio Público en el art. 313, referente al Archivo Fiscal:

Si no se ha podido individualizar al imputado, el Ministerio Público podrá disponer por sí mismo, fundadamente, el archivo de las actuaciones. La investigación podrá ser reabierta en cualquier momento y el plazo para formular el requerimiento fiscal se computará desde la reapertura de la causa.

El archivo se notificará a la víctima que haya realizado la denuncia y solicitada ser informada y ella podrá objetar el archivo ante el juez penal, solicitando una ampliación de la investigación, indicando los medios de prueba practicables o individualizando al imputado.

Si el juez admite la objeción ordenará que prosiga la investigación.

Regimen legal

La Ley n.º 4868/13, “de Comercio Electrónico” en su art. 10 dispone el deber de retención de datos de tráfico relativo a las comunicaciones electrónicas en los siguientes términos:

Los Proveedores de Servicios de Intermediación y los Proveedores de Servicios de Alojamiento de Datos deberán almacenar los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio, por un período mínimo de 6 (seis) meses, en los términos establecidos en este artículo.

Para el cumplimiento de lo dispuesto en este artículo, los datos serán almacenados únicamente a los efectos de facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información.



En ese sentido, deberán almacenar sólo aquellos datos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio.

No podrán utilizar los datos almacenados para fines distintos a los que estén permitidos por la ley, y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos.

La Ley n.º 1682/01, que reglamenta la información de carácter privado en su art. 4.º establece:

Se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables.

Se consideran datos sensibles los referentes a pertenencias raciales o étnicas, preferencias políticas, estado individual de salud, convicciones religiosas, filosóficas o morales; intimidad sexual y, en general, los que fomenten prejuicios y discriminaciones, o afecten la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias.

Convenio de Budapest

La Ley n.º 5994/17, que ratifica el Convenio sobre Ciberdelito del Consejo de Europa, adoptado en la ciudad de Budapest el 23 de noviembre de 2001, además del Protocolo Adicional al Convenio sobre Ciberdelincuencia Relativo a la Penalización de Actos de índole Racista y Xenófobos. Establece en su art.16 la conservación rápida de datos informáticos almacenados, cual expresa lo siguiente:

- 1.Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación.
- 2.Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables.
- 3.Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de dichos procedimientos durante el plazo previsto en su derecho interno.
- 4.Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.



Método

La presente investigación, es de tipo o nivel descriptivo porque comprende la descripción, registro, análisis e interpretación del problema en su naturaleza actual, con enfoque mixto. El alcance está enmarcado a través de la observación directa de hechos punibles ingresados a la Unidad Especializada en Delitos Informáticos del Ministerio Público, de la ciudad de Asunción, que se obtuvieron a través de la oficina de Acceso a la Información Pública acerca de las denuncias realizadas a través del Sistema *Cybertipline* de NCMEC. Así mismo, se realiza entrevistas a encargados de investigar las causas penales de la citada unidad especializada con anterioridad de la Unidad Especializada en Delitos Informáticos del Ministerio Público, localizada en la ciudad de Asunción.

La población de estudio se constituye por; las causas ingresadas a través del Sistema *Cybertipline* desde el año 2014 al 2016, además de los funcionarios encargados de realizar la investigación de las mencionadas causas penales. La muestra es representada por la cantidad de reportes en su totalidad de las causas ingresadas a través del Sistema *Cybertipline*. Finalmente, la entrevista se realizó a través de cuestionarios digitales de *Google Forms*.

Igualmente, la mencionada dependencia proveyó datos referentes a la cantidad de causas que fueron archivadas de conformidad a lo previsto en el art. 313 del CPP. En cuanto a las variables se individualizan; la cantidad de causas ingresadas de pornografía infantil; las dificultades para identificar a los autores y medidas asignadas o adoptadas en relación a las causas penales en las que no se puede identificar al autor.

Análisis de los resultados

Para la presentación de los resultados, se procedió a la observación descriptiva y al relevamiento de informaciones. Los indicadores de las variables expresan los valores en forma absoluta y porcentual, organizados en tablas y gráficos.

Con la técnica de observación directa se realizó un análisis de la cantidad de causas de pornografía relativa a niños, niñas y adolescentes denunciadas mediante el sistema *Cybertipline* de NCMEC.

Conforme al cuadro representativo se puede apreciar que las causas ingresadas por reporte *Cybertipline* de NCMEC fueron distribuidas entre la Unidad Especializada en Trata de Personas y explotación sexual en Niños, Niñas y Adolescentes, que en ese tiempo poseía tres unidades fiscales la n.º 1, n.º 2 y la n.º 3, y la Unidad Especializada en Delitos Informáticos, que en ese tiempo poseía dos unidades fiscales la n.º 1 y la n.º 2. En el año 2014, se señala que fueron ingresadas 247 causas penales en total, al siguiente año la cifra sería más del doble marcando 672, en el año 2016 acaeció con un leve descenso que informa con el número 642 la totalidad de causas ingresadas ese año, el cuadro en solo representa tres años de recepción de denuncias se puede apreciar que ingresaron un total de 1.561 causas penales.



Tabla 1

Cantidad de causas denunciadas ingresadas por Cybertipline en los años 2014 al 2016.

Cantidad de causas denunciadas ingresadas por el sistema Cybertipline			
Año	2014	2015	2016
UFETESI n.º 1	34	181	145
UFETESI n.º 2	57	100	73
UFETESI n.º 3	26	56	120
UEDI n.º 2	65	157	126
UEDI n.º 2	65	178	178
Total	247	672	642
	1561		

Con la técnica de entrevistas utilizada a través del llenado de cuestionarios, realizadas a dieciséis personas y los datos recogidos, se efectuaron los siguientes análisis.

Las respuestas fueron registradas en una base de datos con selecciones múltiples dirigida a funcionarios de la Unidad Especializada en Delitos Informáticos del Ministerio Público. A continuación, se exponen los resultados de las entrevistas realizadas en el marco del trabajo de investigación.

Tabla 2

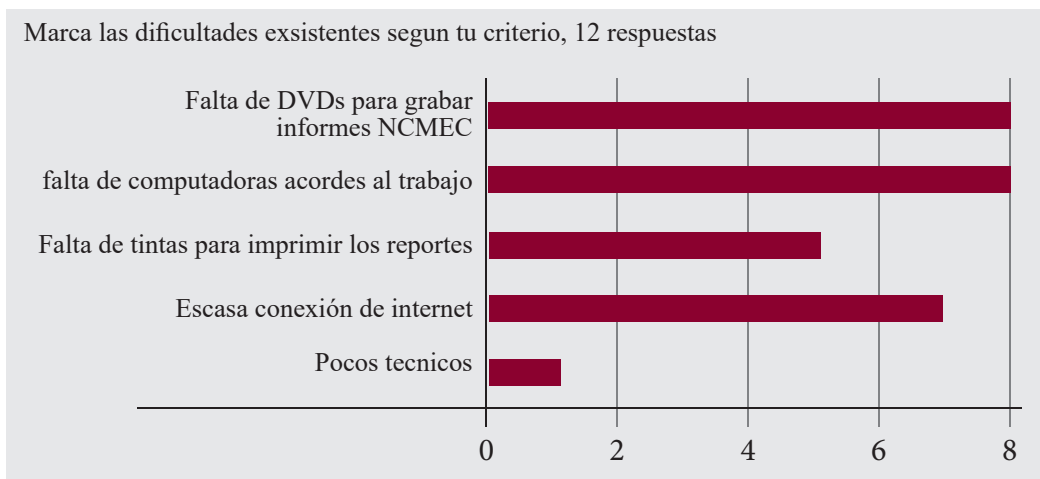
Dificultades con respecto a equipos informáticos.

Pregunta	Respuestas	Encuestados	Porcentaje
¿Existen dificultades con respecto a equipos informáticos en los mencionados casos?	si	12	75%
	no	4	26%
	Total	16	100%

El 75% de los encuestados equivalentes a 12 personas sostuvo la afirmación en la existencia de dificultades con respecto a la relación a equipos informáticos en los casos de pornografía relativa a niños, niñas y adolescentes denunciados a través del Sistema *Cybertipline* de NCMEC.

**Figura 1**

Dificultades existentes relacionadas a equipos informáticos.



En relación a las doce personas que afirmaron la existencia de dificultades referentes a los equipos informáticos en los casos *Cybertipline*, el formulario desplegó opciones para que marquen respecto al tipo de dificultad, las mismas permiten realizar más de una selección. Es así que ocho afirmaron que se requieren DVDs para grabar los reportes de incidentes. Ocho opinaron que se necesitan computadoras acordes al trabajo. Cinco indicaron que es necesario contar con tinta en las impresoras, siete manifestaron que se requiere de una conexión estable a internet. Bajo una sugerencia libre, una persona mencionó que sería apropiado contar con más técnicos en la Unidad Especializada en Delitos Informáticos del Ministerio Público.

Tabla 3

Dificultades con respecto al análisis de los casos.

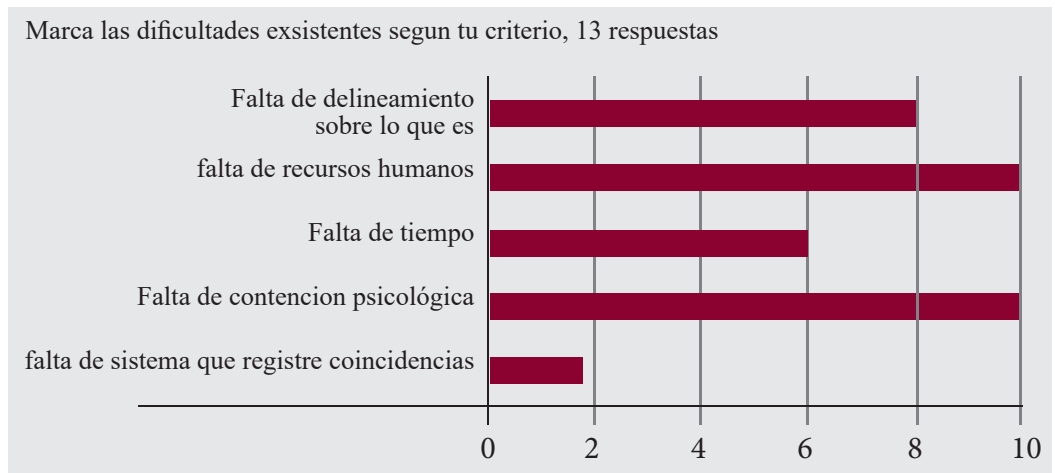
Pregunta	Respuestas	Encuestados	Porcentaje
¿Existen dificultades con respecto al análisis en los mencionados casos?	si	13	81,30%
	no	4	18,80%
	Total	16	100%



El 81,3% de los encuestados equivalentes a 13 personas sostuvieron la afirmación en la existencia de dificultades con respecto al análisis en los casos de pornografía relativa a niños, niñas y adolescentes denunciados a través del sistema *Cybertipline* de NCMEC.

Figura 2

Dificultades existentes relacionadas al análisis de los casos.



Se pudo encontrar que ocho mencionaron la necesidad de delimitaciones de lo que es considerado pornografía, diez indicaron la necesidad de una cantidad mayor de recursos humanos, seis mencionaron que se requiere de más tiempo para el análisis, diez afirmaron que es necesario contar con contención psicológica y una aportó que sería importante contar con un sistema que detecte coincidencias entre reportes.

Tabla 4

Dificultades con respecto a la solicitud de informe de la IP utilizada en los casos.

Pregunta	Respuestas	Encuestados	Porcentaje
¿Existen dificultades con respecto a la solicitud de Informe de la IP utilizada en los mencionados casos?	si	15	93,80%
	no	1	6,30%
	Total	16	100%

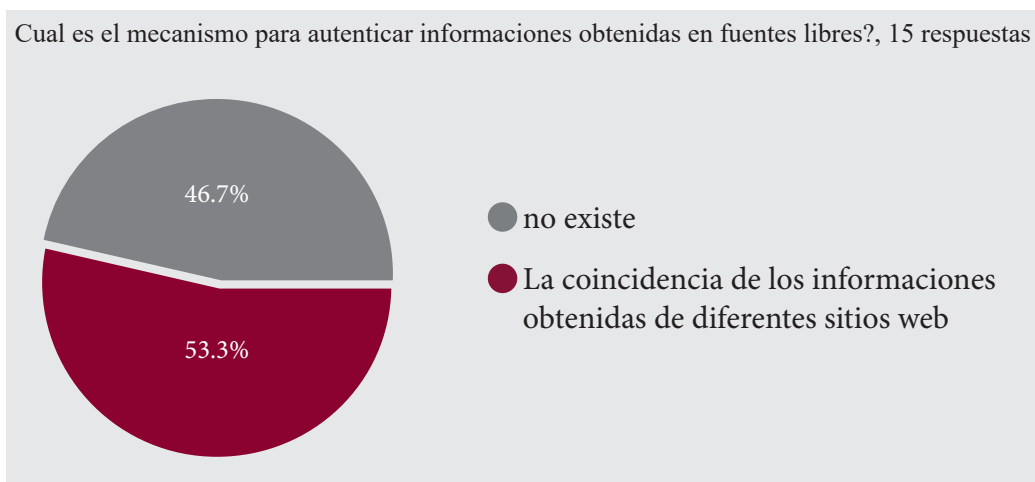


El 93,8% de los encuestados equivalentes a 15 personas afirmaron la existencia de dificultad en respecto a la solicitud de informe de IP utilizada en los casos de pornografía denunciados a través del Sistema *Cybertipline* de NCMEC.

De los cuales catorce indican la existencia de obstáculos en la obtención de la titularidad de direcciones de IP dinámicas y tres manifestaron que desconocen a que empresa corresponde el IP utilizado.

Figura 3

Mecanismo para autenticar informaciones obtenidas en fuentes libres



El 53,3% equivalentes a ocho afirmaron que no existe una forma de autenticar las informaciones obtenidas de fuentes libres y siete equivalente a 46,7% manifestaron que se puede autenticar la información con la coincidencia de las informaciones obtenidas de diferentes sitios web.

Tabla 5

Dificultades con respecto a protocolos de las empresas de telefonía.

Pregunta	Respuestas	Encuestados	Porcentaje
¿Existen dificultades con respecto a protocolos de las empresas de telefonía utilizada en los mencionados casos?	si	13	81, 3%
	no	3	18,80%
	Total	15	100%



El 81,3% de los encuestados equivalentes a 13 personas sostuvo la afirmación en la existencia de dificultades con respecto a protocolos de las empresas de telefonía utilizada en los casos de pornografía relativa a niños, niñas y adolescentes denunciados a través del sistema Cybertipline de NCMEC:

Figura 4

Dificultades existentes con respecto a protocolos de las empresas de telefonía utilizada en los casos



Entre las personas encuestadas que afirmaron la existencia de dificultades en los protocolos de las empresas de telefonía utilizada, se pudo obtener que ocho indicaron que las empresas de telefonía no responden a sus pedidos, catorce manifestaron que tardan en responder, diez afirmaron que las empresas de telefonía no poseen la información solicitada y una remarcó que no están obligadas por ley a responder.

En el año 2014, se señala que fueron archivadas 193 causas penales en total, al siguiente año la cifra sería más del doble marcando 525, en el año 2016 hubo un leve descenso que informa con el número 537 la totalidad de causas ingresadas ese año, del cuadro en solo tres años se puede apreciar que se archivaron 1.255 causas penales.

**Tabla 6**

Cantidad de causas ingresadas por Cybertipline archivadas.

Cantidad de causas ingresadas por Cybertipline archivadas			
Año	2014	2015	2016
UFETESI n.º1	34	176	130
UFETESI n.º2	46	80	58
UFETESI n.º3	15	32	87
UEDI n.º1	63	150	123
UEDI n.º2	35	87	139
Total	193	525	537
	1255		

Conclusión

En cuanto al objetivo general plantado: Establecer los obstáculos que existen en la investigación de los casos de pornografía infantil denunciados a través del Sistema *Cybertipline*, se pudo corroborar en un primer análisis la existencia de dificultades con relación a los equipos informáticos, el análisis de los reportes, las solicitudes de informe de las IPs utilizadas, el mecanismo de autenticación de las fuentes abiertas de información y el protocolo de las empresas de telefonía.

En relación a los objetivos específicos, se denota que entre los años 2014 ingresaron 257 causas, 2015, 672 y 2016, 642, lo que arroja un total de 1.561 causas ingresadas a través del Sistema *Cybertipline*.

Así también, referente a los casos de pornografía infantil en los que no se puede determinar al autor, se destaca que, en el 2014, 193 causas fueron archivadas, en el 2015, 525 y en el 2016, 537, sumando un total de 1.255 causas archivadas de las 1.561 ingresadas.

Sobre la base de los datos expuestos, los números demuestran una realidad inquietante ya que el 80,39% de las causas de pornografía relativa a niños, niña y adolescentes ingresadas a través del Sistema *Cybertipline* de NCMEC son archivadas por falta de identificación del autor.

En relación a las dificultades para identificar a los autores de las causas denunciadas en el periodo de tiempo mencionado, se constató que: se da un déficit en los equipos informáticos de acuerdo a los siguientes datos:



Falta de DVDs para grabar los reportes

Como ya fue expuesto anteriormente en el marco del Convenio de Cooperación Internacional VPN, entre el –NCMEC– y el Ministerio Público de la República del Paraguay, se le otorga acceso a un representante designado de la fuerza del orden, en el caso de Paraguay al coordinador de la Oficina de Apoyo Técnico de la Unidad Especializada en Delitos Informáticos a la red VPN a fin de que realice la extracción de los reportes para su posterior investigación penal.

Una vez extraídos los reportes son grabados en DVDs para su posterior remisión a la unidad penal correspondiente; sin embargo, con el creciente número de reportes y la escasez de insumos, se encuentra un obstáculo al no disponer de suficientes DVDs para grabar todos los reportes.

Falta de computadoras acordes al trabajo

En relación a las computadoras que poseen acceso a la VPN son de número limitado, además, cabe destacar que para el proceso de grabación de reportes deben tener ciertas especificaciones técnicas como reproductor de multimedia, en caso de que el reporte contenga videos y otras aplicaciones que permitan leer el material del reporte y grabador de DVDs.

Falta de insumos como: tinta en las impresoras, hojas etc

Cada reporte del Sistema *Cyberline* cuanta con al menos nueve páginas, ciertos reportes pose en más información y no es raro que lleguen a las sesenta páginas, multiplicando esta cantidad con el número de reportes que existen al año, la cantidad de hojas a imprimir va en aumento, por lo que, contar con la cantidad de tinta para imprimir todos los reportes puede constituir un obstáculo.

Inestabilidad de la conexión a internet

La inestabilidad de la conectividad a internet es un problema que aqueja a todo el país y por consiguiente, también a las instituciones públicas, por lo tanto, puede constituir un obstáculo ya que es el medio para conectarse al sistema y la red de computadoras del Ministerio Público.

Número reducido de técnicos

Actualmente la coordinación de Apoyo Técnico de la Unidad Especializada en Delitos Informáticos cuenta con cinco técnicos para todo el país.

Delineamientos acerca de la pornografía

Existe una disonancia entre el Convenio de Budapest y la Ley n.º 4439/11 de Delitos Informáticos, por un lado, el convenio ratificado por la Ley n.º 5994/17, en su art. 9 sobre delitos relacionados con la Pornografía Infantil establece;

“...2. A los efectos del anterior apartado 1, por «pornografía infantil» se entenderá todo material pornográfico que contenga la representación visual de:

- a) Un menor comportándose de una forma sexualmente explícita;
- b) Una persona que parezca un menor comportándose de una forma sexualmente explícita
- c) Imágenes realistas que representen aún menor comportándose de una forma sexualmente explícita...”



Mientras que la Ley n.º 4439/11, establece en su art. 140 como: “pornografía infantil la representación de actos sexuales con participación de personas menores de dieciocho años de edad o la exhibición de sus partes genitales”. Esta diferencia hace que se reciban reportes que para el Código Penal paraguayo no son considerados pornografía infantil, pero para la legislación internacional sí.

Factor tiempo

Conforme a la cantidad de reportes y el tiempo que debe invertirse en la grabación década reporte en DVDs, es una afirmación muy factible la de apreciar la falta de tiempo como una dificultad.

Contención psicológica

Cada reporte puede contener una o varias imágenes o videos, el material reportado yasea por el valor hash o el *Software Photo DNA*, generalmente consiste en contenido pornográfico infantil, lo cual puede ser muy perturbador y emocionalmente demandante.

Sistema que registre las coincidencias entre reportes

Los reportes están disponibles para el acceso, pero no son procesados ni poseen ninguna clase de filtro, el sistema los hace disponibles y deja a cargo de la fuerza del orden con la jurisdicción correspondiente que haga el análisis.

En cuanto a las dificultades en relación a la solicitud de informe de la IP utilizada, impresiona.

Obstáculos en la obtención de la titularidad de direcciones de IP dinámicas

Algunas telefonías no almacenan datos en relación a las asignaciones de IP dinámicas, esto quiere decir que la dirección cambia con cada conexión a la red, por lo que puede llegar a ser un obstáculo en la investigación de los casos.

Se desconoce a qué empresa corresponde el IP utilizado

Según algunos entrevistados esto se enmarca como una dificultad, sin embargo, existen herramientas totalmente gratuitas que permiten determinar el origen de una dirección de IP.

En cuanto a la autenticación de fuentes abiertas de información, no existe una convergencia sobre la existencia de una forma de autenticar las informaciones obtenidas de fuentes libres.

Las informaciones públicas que se encuentran en internet son consideradas fuentes abiertas de información, las mencionadas según parte de los encuestados no poseen un mecanismo de autenticación y según otra parte se puede autenticar la información con la coincidencia de las informaciones obtenidas de diferentes sitios web.

Por otro lado, se presentan las dificultades en relación al protocolo de las empresas de telefonía que refieren a:

No responden los pedidos: los encuestados afirmaron no obtener respuesta por parte de las empresas de telefonía en relación a las solicitudes de informes realizadas.



Tardan en responder: los encuestados afirmaron que tardan en obtener respuesta por parte de las empresas de telefonía, en relación a las solicitudes de informes realizadas y cabe destacar que las investigaciones deben regirse bajo un plazo.

No poseen la información solicitada: algunas telefonías responden que no cuentan con la información solicitada.

No están obligadas por ley a responder: según la Ley n.º 4868/13, “de Comercio Electrónico” en su art. 10.- Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas, las empresas proveedoras de internet están obligadas a retener el tráfico hasta por seis meses, esto en el marco del comercio electrónico así también la Ley n.º 5994/17, impulsa a las telefonías a retener los mencionados datos. Sin embargo, existe una vaguedad en cuanto al ámbito de las investigaciones penales y la sanción correspondiente por no responder lo solicitado.

Recomendaciones

En relación al promedio de causas ingresadas y archivadas no existe algo que pueda influir en esa cantidad en razón que el actuar del Ministerio Público, se rige por el principio de legalidad establecido en el art.18 del CPP que establece: “...estará obligado a promover la acción penal pública de los hechos punibles que lleguen a su conocimiento” y el art. 313 del mismo cuerpo legal que faculta el archivo fiscal en caso de que no se identifique al autor.

En relación a las dificultades para identificar a los autores de las causas denunciadas en el periodo de tiempo mencionado. Se debería abordar cada dificultad por separado, es así que en relación a las dificultades se especifican de la siguiente manera;

Equipos informáticos; la falta de DVDs para grabar los reportes de incidentes enmarcados dentro de un posible hecho de Pornografía relativa a niños, niñas y adolescentes, la falta de computadoras acordes al trabajo, la falta de tinta en las impresoras, la inestabilidad de la conexión a internet y el reducido número de técnicos. Son problemas mayormente presupuestarios los de insumos, proveedor de servicios de internet y contratos de técnicos. Por lo que deberían ser planteados dentro del estudio del presupuesto.

Análisis; la falta de delineamientos sobre lo que es considerado pornografía, la falta de recursos humanos, la falta de tiempo, la falta de contención psicológica y la falta de un sistema que registre las coincidencias entre reportes. La problemática en cuanto al análisis debería ser abordada oportunamente en un manual de procedimientos que delimite bien los criterios, las tareas, el personal asignado a las tareas y el tiempo que se dedicará a las tareas. Todo para que se puedan filtrar mejor las causas y registrar si existen coincidencias.

Sobre la solicitud de informe sobre la IP utilizada; obstáculos en la obtención de la titularidad de direcciones de IP dinámicas y se desconoce a qué empresa corresponde el IP utilizado. Las operadoras telefónicas del país por lo general, al momento de informar sobre las asignaciones de IP, comunican la imposibilidad de individualizar a los titulares respectivos, debido a la complejidad en el manejo de ese tipo de registro, dado que por su misma esencia aleatoria de utilización se hace imposible la guarda en razón al espacio requerido, por lo que, comúnmente



dicha información no es almacenada en sus sistemas informáticos. Igualmente sea la naturaleza que sea debería de haber un registro que no apañe la impunidad de los hechos punibles cometidos por medios tecnológicos. En relación al desconocimiento de donde provienen las direcciones de IP hay varias herramientas gratuitas en internet que pueden proveer esa información.

En referencia a la falta de mecanismos de autenticación de información obtenida a través de fuentes abiertas, esta problemática siempre va a existir, pero es importante tratar de buscar más datos que puedan reunir suficientes indicios para direccionar una investigación. No se puede confiar ciegamente en las fuentes abiertas, pero se puede realizar variadas búsquedas que recolecten más información para tener un mejor panorama.

En relación a las dificultades referentes al protocolo de las empresas de telefonía; no responden los pedidos, tardan en responder, no poseen la información solicitada y no están obligadas por ley a responder. Es necesaria la promulgación de una ley que obligue a las telefonías a retener datos de tráfico y que establezca las penas por el incumplimiento de remitir informe, así como el incumplimiento en el plazo establecido.

Referencias

- Braganza E. (2013). *Liability And Disclosure Obligations Of Telegraphic And Electronic Service Providers*. Recuperado de <https://ojs.lib.uwo.ca/index.php/uwojls/article/view/5562/4647>
- Eneman M. (2010). Internet service provider (ISP) filtering of child-abusive material: A critical reflection of its effectiveness. *Journal of Sexual Aggression*. Recuperado de <https://doi.org/10.1080/13552601003760014>
- Ley n.º 1286, Código Procesal Penal. Gaceta Oficial de la República del Paraguay, Asunción, Paraguay 14 de julio de 1998.
- Ley n.º 1682 Información de Carácter Privado. Gaceta Oficial de la República del Paraguay, Asunción, Paraguay 19 de enero de 2001.
- Ley n.º 4439 que Modifica y Amplia Varios Artículos de la Ley n.º 1160/97 “Código Penal” Gaceta Oficial de la República del Paraguay, Asunción, Paraguay 05 de octubre de 2011.
- Ley n.º 4868 Comercio Electrónico. Gaceta Oficial de la República del Paraguay, Asunción, Paraguay 01 de marzo de 2013.
- Ley n.º 4868 Comercio Electrónico. Gaceta Oficial de la República del Paraguay, Asunción, Paraguay 01 de marzo de 2013.
- Ley n.º 5994 que aprueba el convenio de Budapest Gaceta Oficial de la República del Paraguay,



Asunción, Paraguay 15 de diciembre de 2017.

Medaris M. y Girouard C. (2002). *Protecting Children in Cyberspace: The ICAC Task Force Program*. Publicado por Office of Juvenile Justice and Delinquency Prevention - Juvenile Justice Bulletin. Recuperado de <https://www.ojp.gov/pdffiles1/ojdp/191213.pdf>.

National Center for Missing and Exploited Children. (2004). *NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN A Powerful Resource for Families, Children and Law Enforcement*. Recuperado de http://betamk.missingkids.com/en_US/documents/nmec_backgroundunder.pdf

National Center for Missing and Exploited Children. (2003) *The CyberTipline: Your Resource for Reporting the Sexual Exploitation of Children*. Recuperado de <https://www.scag.gov/wp-content/uploads/2011/03/cybertip.pdf>

National Center for Missing and Exploited Children (2021) *¿Qué sucede con la información de una CyberTip?*. Recuperado de <https://esp.missingkids.org/gethelpnow/cybertipline>

Reporting requirements of provider 18 U.S. Code 2258A (2008). Recuperado de <https://www.law.cornell.edu/uscode/text/18/2258A>

Sutter, G. (2005). Internet service providers and liability. In M. Klang & A. Murray (Eds), *Human Rights in the Digital Age*. London, UK: Cavendish Publishing.

United States Government Accountability Office (2011) *COMBATING CHILD PORNOGRAPHY*. Recuperado de <https://www.gao.gov/assets/gao-11-33>