Delitos relacionados con la pornografía infantil: Tipología penal, formas de comisión y obstáculos para su investigación en el derecho argentino.

Gonzalo Iglesias, abogado

El presente trabajo analiza el fenomeno de la pornografía infantil por internet, su recepción legislativa y la problematica de su investigación en el derecho argentino

I.- Introducción

Los delitos relacionados con pornografía infantil resultan relativamente nuevos en nuestra legislación, habiendo sido introducido en nuestra legislación en el año 2008 mediante la modificación del art. 128 del código penal por la ley 26.388[i].

Históricamente, la existencia de relaciones entre mayores y menores de edad se remonta a la antigüedad grecoromana. Ariès y Duby, mencionan que la pederastia como una forma de contacto sexual habitual en el imperio romano, actividad tolerada mientras el perpetrador fuera el sujeto activo de la relación[ii]. En el mismo sentido, y durante la época victoriana, movimientos como el uranismo reivindicó dichas practicas sexuales como forma de oposición a la moral imperante.

Desde el punto de vista legislativo, la figura es particularmente reciente, no solo en nuestro derecho, sino también en el comparado. Adler, refiere que no existe un debate de la cuestión hasta a fines de la década de 1970. En Mayo de 1977, un programa de la NBC informaba que aproximadamente unos dos millos de jóvenes americanos se involucraban en la actividad. Estas cifras se reducían sensiblemente en otros medios, como el Chicago Tribune, que estimaba en unos cien mil, los menores involucrados[iii].

El advenimiento de internet constituyó un campo particularmente rico para la acción de los pedófilos. A la fecha, y según datos privados, se estima que en la red existen aproximadamente unos cuatro millones de sitios de material con sexo con menores, creándose aproximadamente unos quinientos en forma diaria. Anualmente, estas páginas reciben un total de dos mil millones de visitas, las que trafican con más de tres millones de imágenes diferentes[iv].

Estos datos, lejos de pasar desapercibidos por la población, han generado una importante preocupación. En una reciente encuesta, el 86 % de los adultos consultados identificó a la pornografía y la pederastía como una de la mayor causa de

preocupación respecto del uso de internet por parte de menores[v]. En similar inteligencia, organizaciones especilizadas en la vistigación de estos delitos señalan a la conducta como uno de los ilícitos de mayor crecimiento en el país.[vi]

Esto ha llevado a una respuesta legislativa tendiente prever y sancionar la conducta. La mayoria de los paises han sancionado leyes criminalizando la actividad y/o han suscripto convenios de cooperación con otros estados o entidades privadas, con el fin de perseguir a los consumidores de pornografía. Sin embargo, debe mencionarse que el resultado de estas modificaciones legislativas son, en muhcos casos, dispares. En un reciente artículo, las autoridades uruguayas refieren que de las quinientas denuncias recibidas por pornografia intantil en el año 2015 solo veintidos habian llegado a procesamiento, proporción que se mantenía en forma constante si se la comparaba con el año anterior (cuatrocientas denuncias contra diecinueve procesamientos)[vii]

En este sentido, debe tenerse en cuenta que mas allá de la adopción de la figura dentro del ordenamiento interno, las formas en que esta se realiza, así como las tecnologías utilizadas para la comisión de la misma tienen un directo impacto en la forma de investigación.

Es el objeto de este trabajo analizar esta problemática y establecer algunas tipologías básicas de comisión con el fin de detectar los problemas y soluciones a adoptar por parte de los operadores jurídicos encargados de legislar y aplicar la figura.

II.- El art 128 del código penal: Breve análisis de la figura y su correlato con el derecho comparado

Mediante la ya referida ley 26388, la República Argentina modificó el art. 128 del código penal, incorporando dos tipos diferenciados que castigan conductas relacionadas con la representaciones sexuales explicitas de menores. La primera es el ofrecimiento, comercialización, publicación, facilitación, divulgación y distribución de representaciones sexuales explicitas que involucren a menores. El segundo tipo penal, previsto con una escala penal sensiblemente menor, es la tenencia de representaciones sexuales explicitas, siempre que la mismas tenga por fin evidente la distribución o comercialización.

En ambos casos, la normativa es tecnológicamente neutra, de forma tal que no importa cuál es el soporte sobre el que se difunda las imágenes. Esto permite la incorporación de los medios informáticos como forma de comisión de este delito, ya sea que estos sean medios de almacenaje magnético (diskettes, discos rígidos), ópticos (cd o dvd) o puramente informáticos, como la distribución mediante redes p2p o servidores

Respecto al objeto material del ilícito, la figura hace referencia a *"toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales"*.

La representacióon puede ser definida como "Imagen o idea que sustituye a la realidad"[viii]. Resulta claro entonces que toda referencia verbal o escrita queda fuera de la órbita de la previsión penal. Respecto a las imagenes simuladas, el proyecto original contemplaba la posibilidad, lo cual fue rechazado por considerar que hacia pasible de impugnación la figura, al avanzar sobre la intimidad de las personas. En este sentido, debe considerarse que en la mayoria de las legislaciones que se ha previsto fue objeto de discusión su constitucionalidad y rechazada[ix].

Respecto de las acciones típicas, el primer párrafo comprende un enunciado exhausitivo de acciones, las cuales pueden dividirse en dos grandes grupos. En el primero podemos encontrar las actividades derivadas de la puesta a disposición del material ya sea a título gratuito (ofrecer, divulgar, distribuir) o claramente oneroso (comerciar). En un segundo grupo encontramos aquellas conductas relacionadas con la creación misma del material: producir, financiar o facilitar. Algunos autores como Carbone[x], han criticado esta solución por entender que resulta redundante ya que en principio el verbo producir incorpora los otros aspectos atento su naturaleza empresarial, mientras que en todo caso el facilitamiento o financiación estaría ya comprendidos como partícipes necesarios del delito atento los principios generales del art. 45 y 56 del Código Penal.

El segundo párrafo preve la tenencia del material siempre que la misma se realice con fines inequívocos de distribución, dejando fuera del tipo penal la tenencia simple del materia. Tal como plantea Gomez, la formulación de la conducta es clara[xi] aunque desde el punto de vista probatorio, la actividad del investigador tiende a complicarse, toda vez que debe probarse la intención de hacer ciruclar el material secuestrado. En este sentido, otras figuras similares como la previsita en la ley de estupefacientes, permiten inferir la voluntad de distribuir en función de las cantidades secuestradas, solución que no es aplicable al caso bajo análisis. Es habitual en los casos de vouyerismo el coleccionismo y clasificación del material mientras que en sentido contrario, aquellas organizaciones dedicadas a la producción de material original carecen de interes en acaparar imagenes de terceros, por lo que la cantidad de representaciones secuestradas tenderá a ser sensiblemente menor al primer caso.

Cabe analizar si la solución de excluir la tenencia simple del tipo penal, tiene un caracter general. Como antecedente inmediato de esta norma debe mencionarse la Convención Internacional de los derechos del niño, tratado incorporado a nuestra constitución en el año 1994, el que establece en su art 34 "*Los Estados Partes se comprometen a proteger al niño contra todas las formas de explotación y abuso sexuales. Con este fin, los Estados Partes tomarán, en particular, todas las medidas de carácter nacional, bilateral y multilateral que sean necesarias para impedir: a) La incitación o la coacción para que un niño se dedique a cualquier actividad sexual ilegal; b) La explotación del niño en la prostitución u otras prácticas sexuales ilegales; c) La explotación del niño en espectáculos o materiales pornográficos.*"

Consecuente con este texto, en el año 2003, se aprobó mediante la ley 25.763, el Protocolo Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de Niños en Pornografía, texto complementario de la convención, obliga a los estados signatarios a la criminalización de la pornografía infantil. En tal sentido, el art 3

establece que los paises signatarios estar obligados a una legislación penal que prevea tanto la producción, como la distribución a titulo oneroso o gratuito, importación, exportación, oferta, venta o posesión con los fines anteriormente señalados de la pornografía infantil.

Sin embargo, esta obligación marca un mínimo en la persecución penal, quedando abierta la posibilidad de que las legislaciones establezcan regulaciones mas severas contra la actividad. En este sentido, la Union Europea ha establecido la directiva 2011/92/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, la que impone en su art 4 párrafo 2 la obligación de los países miembros de adecuar su legislación interna con el fin de castigar con una pena mínima de una año la adquisición y posesión de pornografía infantil[xii]. Este texto marca una diferencia sustancial con el contenido en el Convenio de Cibercriminalidad de Budapest celebrado en el año 2001 en tanto este ultimo permite a los países signatarios la reserva de aplicación de sanciones a la adquisición y posesión de pornografía infantil, tal como surge del parrafo 4 del art. 8 del tratado.

En la actualidad, un total de 71 países prevé en sus legislaciones la tenencia simple de pornografía como delito[xiii]. La mayoría, como figura atenuada de la producción distribución, aunque otros ordenamientos lo preven como una pena similar. En este sentido debe tenerse en cuenta que tanto la legislación federal de EE. UU[xiv]., como de países como Alemania[xv], Inglaterra[xvi] o España[xvii] incluyen la figura en sus ordenamientos.

Esta figura ha sido objeto de controversia entre los autores y organismos intervinientes en la cuestión. Una parte de la doctrina argumenta que la tipificación de la tenencia simple constituye un avance sobre el principio de intimidad, penalizando la elección sexual[xviii]. Otros autores, sin embargo, sostienen la necesidad de su criminalización, atento la defensa de los derechos de los menores involucrados. Entre último grupo podemos mencionar la ONG Internacional Center for Missing and Exploited Children (ICMEC) y la relatora especial de las naciones unidas contra la explotación de menores recomiendan la penalización de la conducta[xix]

Si bien no es objeto de este trabajo analizar las posturas antes mencionadas, debe tenerse en cuenta que la existencia de esta diferencia legislativa afecta directamente la forma en la que la investigación de los hechos se realiza en el ámbito de la instrucción penal.

III.- La investigación penal de la figura. Problemáticas comunes a todos los medios comisivos.

Uno de los problemas preliminares más comunes en el tema de delitos informáticos es la cuestión de la competencia, en particular respecto a si la figura creada debe ser investigada por la justicia local o por los tribunales federales.

En principio, parece claro que, la modificación de la forma de comisión de un delito no debería tener un efecto sustancial en la competencia local o federal. Sin embargo, la irrupción de internet en un principio puso en duda la jurisdicción local de ciertas figuras. Así la propia Corte en autos, *"Embajada Alemana s/Corrupción de menores de 13 años"*[xx] pareció reivindicar la competencia federal en una investigación de pornografía infantil nacida por una comunicación del referido país. Sin embargo, esta postura fue modificada en el año 2008, cuando en una causa de violación del art. 128 del código penal, la corte sostuvo la competencia de un juzgado de garantías local atento el lugar de secuestro de dos discos rígidos con imágenes pornográficas de niños.

Siguiendo a Mayer, la competencia de la justicia federal se encuentra definida por el art. 116 de nuestra carta magna con la expresión "aquellos puntos regidos por la constitución y por las leyes de la Nación, con reserva hecha por el art. 75 inc 12". Si bien la aplicación de este principio será objeto de debate en cada caso concreto respecto a la relativa afectación de los bienes, resulta claro que, en un principio, la competencia por materia se encuentra limitada solamente a las competencias que las provincias en forma expresa delegan en la nación en el texto constitucional, en particular las atribuciones legislativas consagradas en el art. 75 anteriormente mencionado.

En el particular, es importante para este análisis el inciso 14 de referido artículo, en cuanto otorga competencia al gobierno nacional para regular los servicios de correo. Esta clausula ha sido entendida en forma pacífica como comprensiva de todo servicio de comunicación en manos del estado, de lo que se desprende que delitos como la interrupción o la interpretación de correspondencia deben ser competencia federal, con prescindencia del formato en el cual se produce la comunicación.

Por lo expuesto, aquellas figuras que afecten de manera directa el servicio de comunicaciones resultan de competencia federal. Sin embargo, la existencia de un medio comisivo múltiple o una pluralidad de autores no resulta plataforma suficiente para habilitar una competencia de excepción como la federal, sin una afectación de lo establecido por nuestra carta magna

Por lo tanto, debe quedar claro que aquellos delitos comunes en cuya comisión se encuentra involucrada la internet, esta circunstancia no modifica en modo alguno la competencia del órgano destinado a investigarlo. El típico caso de esto son las estafas producidas mediante sitios de remates como MercadoLibre.com o Alamuala.com. En tales casos, la utilización de un medio informático para la comunicación del ardid no modifica en forma alguna la distribución de competencia, la que quedan en manos de la justicia local, tal como lo ha sostenido en forma reiterada la propia Corte Suprema de Justicia en causas como *Cybernetics y otro s/estafa*[xxi] o *Fava Esteban Eduardo y otros s/Estafa*[xxii] entre otras. En estos casos en que se está frente a una territorialidad difusa, donde resulta difícil establecer el lugar de consumación del ilícito, es habitual adoptar un criterio de economía procesal, permitiendo que el juzgado previniente continúe la instrucción de la causa.

Sin embargo, es necesario hacer notar que, en la mayoría de los casos de investigaciones de pornografía en el país, la dirección IP desde donde se subió el archivo, se encuentra individualizada en la denuncia, por lo que la competencia en tal caso se encuentra determinada por la dirección física otorgada a la misma, tal como surge de lo sostenido por la Corte Suprema en autos "Eslaiman, Alicia s/ infr. ley 11.723"[xxiii].

Un segundo problema es la dependencia de los agentes judiciales respecto de la colaboración de entidades privadas. Particularmente al principio de la investigación, es habitual que los datos identificatorios de los autores se encuentren en poder de entidades privadas, ya sea en forma de registros de conexiones, listados de ips o perfiles de usuarios. Esta circunstancia conlleva dos problemas para investigación: El primero la conservación misma de estos datos y en segundo lugar, la forma de acceso a los mismos, en los casos que los particulares sean empresas multinacionales.

La conservación de los datos no es una cuestión menor. Entidades como ICMEC establecen como requisito necesario de una regulación adecuada de protección contra el delito una política de resguardo de los datos[xxiv]. En el mismo sentido la legislación europea ha regulado el tema mediante la directiva 2006/24/CE sobre conservación de datos de tráfico y de localización telefónicos y de comunicaciones, que establece la obligación de los prestatarios de servicios de telecomunicaciones de conservar los datos de tráfico por el término de 6 a 24 meses según lo disponga la legislación de los países miembros.

Desde el punto de vista del derecho internacional público, el Convenio sobre Cibercriminalidad de Budapest establece en su art. 16 la obligación de los países miembros de prever la conservación de los datos de tráfico, así como arbitrar los medios para compelir a los particulares a su resguardo y comunicación en casos de delitos graves.

En nuestro país, la ley 25.873[xxv] modificó la ley 19.728 incorporando dos artículos identificado como *45 bis y ter* regulando la captación y derivación de comunicaciones para su observación remota por parte de organismos de seguridad, estableciendo la obligación de los proveedores de internet de mantener los datos de tráfico por el término de diez años.

Esta norma fue impugnada en re *"Halabi c/PEN s/Amparo"*[xxvi], fallo de Corte Suprema que acogió por primera vez una acción colectiva en la jurisprudencia argentina. Respecto al tema de la constitucionalidad, el Supremo Tribunal resuelve en contra de la validez de la norma argumentando que las misma invade los derechos consagrados en el art. 18 de la constitución.

El fallo ha sido objeto de críticas por parte de la doctrina especializada. Tanto Horacio Fernadez Delpech[xxvii] como Pablo Palazzi[xxviii], ambos en ocasión del fallo de cámara finalmente ratificado por el Superior Tribunal, criticaron el criterio adoptado, por entender que ponía en riesgo herramientas fundamentales para la investigación de delitos cometidos mediante medios informáticos. Mas allá de estas observaciones, las que el autor de la presente comparte, resulta claro que, en la actualidad, existe en este

sentido un vacío legal respecto a los plazos de conservación de los datos en el derecho argentino.

La segunda problemática respecto a los particulares es la forma de acceso a estos datos con las que cuenta el operador judicial. En muchos casos, las empresas multinacionales prestatarias de servicios se niegan a responder los oficios dirigidos a sus oficinas locales, argumentando que tales sucursales tienen solo una función comercial, siendo necesaria la via de exhorto internacional para acceder a estos datos.

Si bien desde el punto operativo, esto supone un freno a la celeridad de las investigaciones, implica asimismo una limitación de la soberanía del estado, en tanto son los particulares los que establecen la forma y contenido de la obligación de contestar las requisitorias, al establecer las sedes encargadas de contestar las mismas. En este sentido la guía de Law Enforcement del sitio facebook.com establece que "la revelación de registros de una cuenta solo puede hacerse de confirmidad con nuestras condiciones de servicio y ley pertinente"[xxix]

Recientemente esta cuestión fue objeto de pronunciamiento judicial en sede civil, rechazando la limitación planteada por el particular. En CEA c/ Google Inc. S/habeas data[xxx], la Cámara Nacional de Apelaciones en lo Civil y Comercial, Sala III rechazó la negativa de la firma Google de utilizar el exorto como forma para obtener la información requerida en el proceso. En este sentido el tribunal ha sotenido que "*no puede entenderse -en este estado preliminar con el único argumento expuesto someramente por Google a fs. 164/vta.- que el pedido de la autoridad judicial competente al que se refirió la empresa en las mencionadas cartas documento, deba ser formulado por exhorto diplomático a los Estados Unidos por encontrarse ubicados en dicho país los servidores en los cuales está alojada la información, cuando los efectos dañosos se verifican en la jurisdicción de este Tribunal"* En el mismo sentido luego agrega que *"Es que en una aproximación al tema -apropiada al estado del pleito- no puede soslayarse que la ratio de la regulación legal acerca del emplazamiento de las sociedades extranjeras es la de evitar elusiones o dilaciones formales o procesales basadas en la dificultad práctica y mayores costos (en ese sentido, cfr. esta Cámara, Sala 2, doctrina de la causa 4913/13 del 8-7-2015 y sus citas de doctrina). En suma, tratándose del cumplimiento de un requerimiento judicial para dictar una decisión acerca de la medida cautelar que compatibilice una tutela rápida y eficaz de los derechos personalísimos del actor con la menor afectación posible de las demás garantías constitucionales involucradas en el sub examine (vgr. la libertad de expresión en su faz individual como colectiva), no es admisible la decisión recurrida desde que es contraria a los fundamentos y principios precedentemente expuestos; ello importaría una demora y un costo que no está justificado con la respuesta de Google Inc."*

Si bien esta solución se da en el marco de un juicio civil, es opinión del autor que las consideraciones que la fundan pueden ser aplicación a cualquier requerimiento judicial, con prescindencia de la materia que se debata en el proceso.

IV.- Formas modernas de comisión del delito. Redes Peer to Peer y Deep Web.

Aunque, tal como mencionamos anteriormente, la regulación de la figura es tecnológicamente neutra, el delito va variando en sus forma de comisión, en busca de técnologías que permitan el mayor anonimato posible para sus autores.

En este sentido, debe mencionarse que, en la actualidad, las formas mas usuales de distribución son las redes peer to peer y en recientemente las redes anonimizadas conocidas como deep web, fenómenos tecnológicos que presentan sus propias características y problemas para la investigación.

La utilización de redes peer to peer (p2p): La posibilidad de distribución y su prueba forense

Podemos definir a una red informática entre iguales (en inglés, peer- Too -peer -que se traduciría de par a par- o de punto a punto, y más conocida como P2P) como una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red. Esta arquitectura presenta una serie de beneficios como sus estabilidad y robustez al encontrarse los datos distribuidos en forma uniforme en multitudes de máquinas. Asimismo, y esto no es un tema menor, implica una reducción de costos al utilizar a los mismo usuarios para solventar elementos como el almacenaje o ancho de banda.

Desde el punto de vista de su estructura las redes P2P pueden ser centralizadas, semicentralizadas o descentralizadas. En una red centralizada un servidor central que registra y modera las transacciones entre los usuarios. En la red semicentralizadada el servidor central que sirve como *hub* y administra los recursos de banda ancha, enrutamientos y comunicación entre nodos pero sin saber la identidad de cada nodo y sin almacenar información alguna, por lo que el servidor no comparte archivos de ningún tipo. Por ultimo en una red descentralizada, la figura del servidor central desparece, siendo suplantado por los propios usuarios que se conectan directamente, utilizando los recursos de otro usuario como nodo.

La mayoría de las redes en funcionamiento se encuentran en los últimos dos grupos, imponiendo en la actualidad las redes descentralizadas como forma de estructura típica. Desde el punto de vista legal, esto derivó en la disputa respecto a la responsabilidad de los creadores de las redes respecto a las actividades de sus usuarios, tema que hoy día siguen en debate[xxxi]. Desde el punto de vista de la investigación resulta claro que un requerimiento al gestor de las redes resulta a todas luces infructuoso, habida cuenta que carece de conocimiento respecto de la identidad y actividades de sus usuarios.

Atento ello, las autoridades y ONG interesadas optaron por controlar los archivos y direcciones IP involucradas. Respecto de los archivos la utilización de algoritmos hash permite identificar los materiales ilicitos que circulan por la red y en caso de encontrarlos establecer las direcciones IP involucradas en el intercambio.

En general, una vez recibida la denuncia de intercambio , el investigador judicial solicita prueba de informes con el fin de asociar la dirección IP a un domicilio físico determinado. Conseguida esta, y mediante una orden de allanamiento de juez competente, se accede al domicilio, secuestrandose el material informático que allí se encuentre para su posterior análisis forense .

Marc Liberator, Brian Neil Levine y Clay Shields[xxxii] plantean un problema con esta forma de trabajo atento la utilización de la dirección IP como elemento básico del proceso. Por su propia naturaleza, la IP tiene una serie de limitaciones en cuanto la prueba del ilícito. En principio, toda dirección registrada no tiene en cuenta la existencia de redes internas dentro del domicilio o la utilización de dispositivos móviles como telefonos o tablets. Violaciones de seguridad de la ya mencionada red o la instalación de troyanos obtendrían un falso positivo respecto del autor del ilícito, con el subsiguiente perjuicio . Asimismo, la mera existencia de una comunicación carece de poder convictivo respecto de la intención de cometer el ilícito.

Respecto a la presencia de redes dentro del domicilio, es un elemento a tener en cuenta al momento de realizar el allanamiento. En particular, al secuestrar el material es necesario no solo identificarlo sino también establecer su procedencia, de forma tal de poder vincular, de ser posible, el ordenador con un usuario determinado. En este sentido, la mayoría de los protocolos de actuación pericial aprobados o en proyecto, prevén la necesidad de esta operación, ya sea mediante fotografías, croquis o identificación de los usuarios asignados a cada computadora[xxxiii].

Respecto a la labor pericial, existen en el mercado numerosas soluciones informáticas que permiten identificar el material pornográfico infantil. En particular el Griffeye Analyzer, programa que se licencia en forma gratuita a los organismos que investigan casos de pornografía infantil, permite reconocer dada una imagen de disco, aquellas imágenes carentes de interés forense (vg logotipos o íconos del sistema operativo) de aquellas imagenes ya previamente identificadas como pornografía infantil mediante su valor hash. De esta manera, libera al perito de una carga sensible de trabajo, permitiéndole concentrarse en aquellas imágenes sin catalogar ya sean estas material sin interés para la causa o imágenes pornográficas inéditas.

Sin embargo, esta solución solo permite establecer la posesión de dicho material pero no su distribución. Si bien esto es una solución aceptable en muchos países[xxxiv], tal como ya se analizó el derecho interno argentino no prevé la mera posesión como delito, debiendo por tanto acreditarse la distribución del material o por lo menos su tenencia con dicha intención. Esto reviste particular importancia, toda vez que en la mayoría de los casos, si bien se recupera gran cantidad de material pornográfico infantil, por el tiempo transcurrido el archivo que dió lugar a la demanda puede haber sido removido de la máquina.

A estos efectos, debe tenerse en cuenta que la utilización de una red P2P implica la posibilidad por parte del usuario no solo de obtener el material sino al mismo tiempo funciona como un servidor del restos de la red. Esto obedece a que al momento su distribución, todo archivo es dividido en partes, a las cuales los usuarios acceden en forma indistinta hasta completarlo, siendo unido por el programa de

gestión de la red en la máquina de destino. Por lo tanto, cada usuario de una red p2p técnicamente se encuentra distribuyendo el archivo al mismo tiempo en que se encuentra bajandolo.

La pregunta desde el punto de vista jurídico es si este distribuir puede ser considerado una acción típica dentro de nuestro ordenamiento. En este sentido debemos precisar que, si bien las carpetas se encuentran abiertas a los demás miembros de la red, los usuarios en cualquier momento pueden negarse a compartir el material sea en todo o en parte. Sin embargo, la mayoría de las redes castigan esta posibilidad, limitando la prioridad de dichos usuarios para acceder a los archivos mas requeridos y por tanto alargando los tiempos de descarga de los mismos.

En este sentido, la jurisprudencia española ha establecido en numerosas oportunidades que la utilización de estas redes constituye un mecanismo de distribución. En tal sentido el fallo de casación rechaza la pretensión del acusado respecto a encuadrar la figura dentro del delito posesión para uso privado bajo el fundamento que *"...en primer lugar, el sistema Emule del que se valía para descargar los archivos de Internet y acopiar en su ordenador el material pornográfico se basa en el intercambio de archivos, de modo que cuantos más comparta más puede almacenar. Y lo cierto es que el acusado poseía casi tres mil archivos, dato que constituye un importante indicio de que compartía sus archivos con otros internautas de la Red, ya que es la única forma de conciliar razonablemente la reciprocidad del programa con la importante cifra de material pornográfico almacenado por el acusado.*

En segundo lugar, cuando operaba con la carpeta de entrada ("incoming") su ordenador compartía sus archivos con otros internautas, pues para poder descargar en su carpeta de entrada precisa tener accionada la velocidad de salida, aunque sea al mínimo. De ahí que, aunque redujera el número de archivos que subía o reenviaba a otros internautas, es claro que siempre existía un número mínimo de archivos reenviados cuando operaba con la referida carpeta.

Por último, en la sentencia recurrida se declara probado que el acusado cursó estudios de electrónica a nivel de FP 2. Tras acceder a la página Emule, se descargó el programa y lo instaló en su PC. Además, instalaba los antivirus y formateaba su ordenador. También descargó e instaló el programa "Nero" destinado a copiar y enviar archivos y datos desde el disco duro del ordenador hasta los CD's o los DVD's.

La concurrencia de estos indicadores externos permite inferir que el acusado sabía perfectamente que con el uso del programa EMULE estaba facilitando la difusión de los vídeos pornográficos que descargaba en su ordenador, dada la mecánica específica del sistema que aplicaba. Pues una persona que tiene los conocimientos y experiencia en informática del acusado tiene que ser sabedor de la forma en que opera el programa que aplica, los efectos que produce y las derivaciones hacia terceros. Si a ello se la añade su uso reiterado y el almacenamiento de los archivos que obtenía, debe colegirse que conocía lo que ejecutaba informáticamente y

asumía o aceptaba las consecuencias de su conducta, esto, es la difusión del material pornográfico a otros usuarios de la Red"[xxxv]

Sin embargo, la mera presencia de un sistema de P2P no puede establecer en forma automática la existencia de una distribución. La propia jurisprudencia española en numerosas oportunidades ha rechazado la pretensión fiscal al argumental la falta de prueba de la intención del agente. Asi en el Recurso 79/2011, AP Valencia, Sec. 3.ª, 93/2012, del 9 de febrero del 2012, se entendió que la ausencia de grandes cantidades de archivos recuperados, asi como el desconocimiento por parte del autor de la técnica informática no permitían sostener el delito de distribución[xxxvi].

Desde el punto de vista forense, esta observación implica la necesidad de recuperar nuevos elementos del material secuestrado, en particular respecto al historial de uso. Existen en el mercado, varios programas forenses que registran los cambios en la configuración de el cliente de la red como el Internet Evidence Finder u otros de carácter mas general como el Encase que tambien puede cumplir dicha función. En particular las modificaciones al ancho de banda disponible para subir los archivos, la cantidad de conexiones simultaneas o la remoción de los archivos de la carpeta compartido hacia un disponitivo externo u otra carpeta dentro del mismo rígido son indicios claros del conocimiento por parte del usuario del funcionamiento del sistema. Asimismo debe tenerse en cuenta que en los programas mas usados existe la posibilidad de determinar cuales son los archivos a compartir y cuales no. Esta opción deja rastros en la configuración del sistema que pueden ser recuperados por software forense como autopsy o los ya mencionados constituyendo un elemento claro del conocimiento del autor de la comisión de la conducta ilícita.

La deep web y la utilización de agentes encubiertos

Es una características de los consumidores de pornografía infantil vía web la adopción temprana de tecnologías que aseguren el anonimato de los usuarios. En particular, en los últimos años, se ha visto una marcada utilización de mecanismos o soluciones basadas en la llamada dark web.

Entendemos por Dark Web a aquella parte de la red global cuya navegación requiere la utilización de protocolos o programas especiales destinados a oscurecer la identidad y/o actividad de sus usuarios. El programa mas utilizado o conocido popularmente es TOR acrónimo para The Onion Router. Dicho software utiliza mecanismo de encriptamiento respecto a la IP del usuario, la que pasa por un circuito de relays elegidos en forma aleatoria. De esta forma la IP de origen queda eclipsada por una serie de capas de desviaciones protegidas por criptografía (de ahi la utilización de la analogía con la cebolla) lográndose el pretendido anonimato.

En un reciente estudio de la Universidad de Portsmouth[xxxvii], estableció que casi el ochenta por ciento de las visitas producidas en la dark web correponden a requitorias en páginas de pornografía infantil o éticamente discutible (aquella que representa acciones no consensuales o zoofilia). Muchos de estos sitios imponen restricciones con el fin del intercambio de archivos: en particular es habitual que el

nuevo usuario ponga disposición material propio o incluso inédito para su inclusión. Esto permite un doble objetivo: El primero renovar la oferta de material para los consumidores de la página y en segundo lugar limitar el acceso a aquellas personas que, en principio, hayan cometido el ilícito a investigar.

Frente a esta realidad, la forma de investigación debe necesariamente variar. En el año 2015, una operación del FBI identificó un total de 1300 usuairios del sitio playpen, pagina de la dark web con servidor con sede en Carolina del Norte. Si bien el servidor fue requisado en el mes de febrero de 2015, la agencia de investigaciones estadounidenses siguió operando el sitio, con el fin de hackear los ordenadores de los usuarios que se conectaban a la misma[xxxviii].

En la misma inteligencia varios países de Europa comienzan a legislar la figura del agente encubierto informático. España mediante la ley organica 13/2015 de octubre de dicho año, modificó su código de enjuiciamiento incorporando la figura en los párrafos 6 y 7 del art. 282 bis con la siguiente redacción: *«6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a. El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos. 7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio"*.

Si bien la figura aparece como una herramienta necesaria para investigación de ilícitos como el analizado, cabe preguntarse en el caso de adoptarse en nuestro ordenamiento cual sería su recepción por parte de la jurisprudencia y la doctrina nacional atento el avance sobre la intimidad de los particulares y la posibilidad, cierta atento su ocurrencia en otros casos de investigaciones encubiertas, que el agente sobrepase los límites impuestos transformándose en provocador de la conducta ilícita que pretende investigar.

V.- Conclusiones

1.- Resulta claro que el fenómeno de la pornografía infantil y su investigación constituye un fenómeno cambiante y complejo, haciéndose necesario su abordaje mediante una óptica multidisciplinaria, siempre teneindo en cuenta los tipos penales legislados en cada ordenamiento

2.- Al mismo tiempo, es necesario por parte de los operadores jurídicos como fiscales o instructores, últimos responsables de la investigación penal, un

conocimiento técnico mínimo para guiar el accionar de los peritos. En el mismo sentido resulta primordial la presencia de estos últimos o, en su defecto, la confección de protocolos de actuación nomalizados, a los efectos de la recolección de la prueba con el fin de evitar nulidades o pérdida de elementos de convicción.

3.- El cambio tecnológico obliga a abordar las investigaciones en forma novedosa atento la irrupción de tecnologías disruptivas.

3.1.- En particular resulta primordial la regulación del acceso de los datos en poder de perticulares en el ámbito internacional, a los efectos de evitar las dilaciones derivadas de la utilización de un método como el exorto, a todas luces incompatible con los tiempos procesales de una investigación.

3.2.- Respecto a la utilización de redes P2P, resulta necesario la adopción de criterios particulares para la investigación en paises como Argentina, que no contempla la figura de la tenencia simple, lo que hace poco conveniente la adopción de metodologías de análisis desarrolladas en paises que preven el tipo penal.

3.3.- Por último, la derivación de la actividad hacia páginas anonimizadas hace necesaria que la doctrina, la jurisprudencia y la legislación comienzen a analizar nuevas figuras investigativas como el agente encubierto o la utilización de programas remotos, herramientas que si bien constituyen medios eficientes de adquisición de prueba, comprometen garatías básicas del proceso penal.

iSancionada el 4 de Junio de 2008, promulgada de hecho el 24 de Junio de 2008.

iiAriès y Duby (directores) Historia de la Vida Privada, Tomo I, Pags. 200 y sigs., Ed Taurus, 1991

iiiAmy Adler, *The Perverse Law of Child Pornography, Columbia Law Review, 2001.*

ivFundación Anesvad *Informe Sobre la Pornografía Infantil en Internet,*

vEncuesta realizada por la firma ESET Latinoamérica en fecha 21 de octubre del 2011, disponible en www.eset-la.com

vihttp://www.ambito.com/836974-pornografia-infantil-y-fraude-bancario-los-principales-delitos-informaticos

viihttp://www.infobae.com/2015/10/28/1765513-uruguay-registro-500-casos-pornografia-infantil-2015

viii Definición del Diccionario de la Lengua, Real Academia Española, versión en línea en "http://dle.rae.es/?w=diccionario"

ix En particular el fallo "Ashcroft vs Free Speech Coalition", disponible en https://www.law.cornell.edu/supct/html/00-795.ZO.html

x Carbone, Diego, "Comentarios a la ley de delitos informáticos, 26.388, Nuevos delitos, Viejos delitos", disponible en ar.Microjurisc.om

xi Leopoldo S.M. Gomez, El delito de pornografía infantil, Ad Hoc, Buenos Aires, 2012

xiiPromulgado el 13 de diciembre de 2011. Texto disponible en español en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011L0093&from=HR

xiiiChild Pornography: Model Legislation and Globa Review, 8 edition, Internacnional Center for missing and exploited children, 2016 disponible en http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf

xiv18 U.S. Code § 2252 - Certain activities relating to material involving the sexual exploitation of minors, prevé un mínimo de 10 años por posesión, pena que se agrava en el caso de reincidentes o desscripción de ciertas conductas violentas.

xvEl artículo 183.5 del Cóigo Penal Aleman castiga a quien procure conseguir para sí o para un tercero la posesión de publicaciones pornográficas (§ 11 inciso 3), que tengan por objeto el abuso sexual de niños, cuando las publicaciones reproduzcan un suceso real o cercano a la realidad

xviSe prevé como posesión de una fotografía indecente de un menor. El acusado pueda defenderse argumentando que tiene un motivo legítimo de poseer ese documento, que no lo ha visto el mismo y que no conoce su contenido, o que lo ha recibido sin haberlo solicitado y que no lo ha conservado más allá de un de plazo razonable. Hasta la reforma procesal del año 2000, este delito era sancionado con una multa y/o con una pena de cárcel de una duración máxima de seis meses . Luego de la reforma el período de cárcel puede alcanzar cinco años

xviiEl art 189 quinto párrafo del código penal español preve la figura atenuada de posesión simple, con una pena de multa o tres meses a un año de prisión.

xviiiEntre otros Dra. Laura Mayer Lux, Almacenamiento de pornografía en cuya elaboración se utilice a menores de dieciocho años: un delito asistemático, ilegítimo e inútil , Polít. crim. Vol. 9, Nº 17 (Julio 2014), Art. 2, pp. 27-57, disponible en http://www.politicacriminal.cl/Vol_09/n_17/Vol9N17A2.pdf

xixEn particular ver Informe de la Relatora Especial sobre la venta de niños, la prostitución infantil y la utilización de niños en la pornografía de fecha 30 de diciembre de 2015, disponible en https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/294/67/PDF/G1529467.pdf?OpenElement

xx Competencia N° 1540. XLI, fallada el 27 de diciembre de 2005, disponible en http://www.csjn.gov.ar/confal/ConsultaCompletaFallos.do?method=verDocumentos&id=598330

xxi El fallo adhiere a los fundamentos del dictamen de Procuración disponible en http://www.mpf.gov.ar/dictamenes/2011/GWarcalde/octubre/C_y_Otro_Comp_695_L_XLVII.pdf

xxiiIdem anterior. Dictamen disponible en http://www.mpf.gov.ar/dictamenes/2011/GWarcalde/junio/F_Esteban_Comp_343_L_XLVII.pdf

xxiiiS.C. Comp. 888, L. XLV. Disponible asimismo en http://servicios.csjn.gov.ar/

xxivChild Pornography: Model Legislation and Globa Review, 8 edition, Internacnional Center for missing and exploited children, 2016 disponible en http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf

xxvPromulagada Febrero 6 de 2004 disponible en http://infoleg.mecon.gov.ar/infolegInternet/anexos/90000-94999/92549/norma.htm

xxviSentencia de la Suprema Corte de la Nación de fecha 24 de febrero de 2009. Dispobible en http://www.habeasdata.org/wp/2009/02/24/fallo-corte-datos-de-trafico/

xxviiHoracio Fernandez Delpech, *"La conservación de los datos de tráfico en la lucha contra la delincuencia informática"*, Universidad Autónoma de Mexico

xxviiiPablo Palazzi, *"La controversia sobre la retención de datos de tráfico en Internet"*, La Ley 28 de abril del 2005.

xxixDisponible en Https://www.facebook.com/safety/gruops/law/guidelines

xxxFallo de fecha 29 de septiembre de 2015

xxxiAl respecto, Sanchez Iregui, Felipe, DE LA ILEGALIDAD DE NAPSTER A LA LEGALIDAD DE KAZAA, GROKSTER, GNUTELLA Y STREAMCAST , disponible en http://alfa-redi.org/sites/default/files/articles/files/sanchez.pdf

xxxiiMarc Liberatore◦ Brian Neil Levine◦ Clay Shields, Strengthening Forensic Investigations of Child Pornography on P2P Networks , disponible en http://conferences.sigcomm.org/co-next/2010/CoNEXT_papers/19-Liberatore.pdf

xxxiiiEn particular ver el Protocolo de Actuación para Pericias Informáticas de la Provincia de Neuquen disponible en http://www.jusneuquen.gov.ar/images2/Biblioteca/ProtocoloActuacionPericiasInformaticas.pdf

xxxivGriffeye y su antecedente netclean se distribuían en forma gratuita y contaban con un convenio de colaboración con ICMEC, ONG con sede en los EE UU.

xxxvSentencia T.S. 1299/2011 (Sala 2) de 17 de noviembre de 2011, disponible en http://portaljuridico.lexnova.es/jurisprudencia/JURIDICO/135396/sentencia-ts-1299-2011-sala-2-de-17-de-noviembre-facilitacion-de-la-difusion-de-pornografia-in.

En el mismo sentido, ver Sentencia T.S. 30/2011 (Sala 2) de 7 de febrero, disponible en la misma dirección

xxxvi Disponible en http://www.sepin.es/servicios_n/

xxxviihttps://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/. Asimismo puede verse la exposición de dicho trabajo por su autor, Dr Gareth Owen en https://www.youtube.com/watch?v=-oTEoLB-ses&feature=youtu.be&t=1998

xxxviiiLa forma y fudamentos de dicha operación pueden verse en **US. v. Ferrell - Affidavit in Support of Search Warrant** , disponible en https://www.documentcloud.org/documents/2165971-us-v-ferrell-affidavit-in-support-of-search.html