Nuevas herramientas de investigación penal: el agente encubierto digital

Abog. Marcelo Temperini[1] y AIA Maximiliano Macedo[2]

Introducción

Para combatir delitos cada vez más complejos, y sobre todo cuando intervienen las nuevas tecnologías como medio para la comisión de los mismos, el Estado necesita adaptarse y actualizarse. En general, así concluyen los distintos trabajos y eventos relacionados con la delincuencia informática y cibercrimen, donde se muestran nuevas técnicas y modalidades utilizadas por los delincuentes que utilizan las tecnologías de la información y las comunicaciones para su propio beneficio.

No es novedad afirmar que el contínuo avance de las tecnologías trae consigo nuevos desafíos y amenazas. En el ámbito de la delincuencia, el crecimiento en la utilización de Internet brinda un abanico nuevas formas y medios sobre los cuáles cometer delitos, aprovechándose de usuarios que diariamente acceden a Internet desde todo tipo de dispositivos (smartphones, tablets, notebooks, entre otros). Este escenario trae como consecuencia un aumento de la población pasiva que potencialmente puede ser víctima de distintos tipos de ataques, aumentando las posibilidades para los delincuentes que utilizan la tecnología para llevar a cabo sus acciones.

El presente trabajo, pretende en primera instancia repasar los desafíos actuales que tienen las fuerzas de seguridad al momento de llevar a cabo una investigación penal sobre delitos cometidos a través de medios informáticos o bien, cuyo objeto del delito es la información. Desde ese escenario, los autores se plantean la necesidad de la incorporación de la figura del agente encubierto digital, como una herramienta de investigación, limitado en principio, a que un agente de las fuerzas de seguridad pueda, a través de medios electrónicos, ocultar su identidad para conseguir obtener información útil para el avance de investigaciones de aquellos delitos donde el bien jurídico afectado sea la integridad de un menor.

Tecnología y Delitos

La tecnología es neutra. Pero dicha neutralidad, puede volverse positiva o negativa de acuerdo a la forma de utilización que hagan las personas. La proliferación de sistemas vulnerables, combinado con un incremento de usuarios de escasos conocimientos técnicos que se suman a la nueva generación de redes como Facebook, Twitter, Whatsapp, Instagram, SnapChat, entre otros, en combinación con la posibilidad de llevar adelante ataques de forma masiva e instantánea desde distintos lugares del mundo, sumado a las distintas técnicas y tecnologías que brindan en mayor o menor medida el anonimato, generan para el mundo de la

1 Abogado (UNL) especialista en Derecho Informático. Doctorando CONICET dedicado a la investigación de Delitos Informáticos y Cibercrimen (FCJS / UNL). Socio Fundador de AsegurarTe www.asegurarte.com.ar. Miembro de la Comisión Directiva de ADIAr. Co-fundador del Proyecto ODILA: Observatorio de Delitos Informáticos de Latinoamérica. Contacto: temperinimarcelo@gmail.com

2 Analista en Informática Aplicada (FICH UNL), Especialista en Seguridad Informática. Socio fundador de AsegurarTe - Consultora en Seguridad de la Información. Participa activamente en diversos congresos, exposiciones y proyectos destacándose entre ellos: “Conciencia Digital”, “Proyecto ODILA: Observatorio de Delitos Informáticos de Latinoamérica” y “Botón de Pánico AsT” | Contacto: mmacedo@asegurarte.com.ar

delincuencia informática una oportunidad sin igual para llevar adelante toda una variedad de delitos, desde los más simples hasta los más complejos y organizados.

Si bien es posible encontrarse con delincuentes informáticos que actúan de forma independiente o aislada, lo cierto es que la complejidad de algunos delitos requieren un cierto nivel de organización, algo que puede observarse cada vez más en la red de redes. De acuerdo a un estudio realizado por Panda Security [1], las mafias de ciberdelincuentes que operan en Internet están muy organizadas, tanto desde el punto de vista de visión estratégica como desde la operativa, logística y despliegue de sus operaciones.

De este último informe, se ha extraído una clasificación publicada por el FBI, de las diferentes "profesiones o especializaciones" del mundo de los cibercriminales, en un intento de tipificar las figuras más comunes que podemos encontrar en estas bandas que en algunos casos se dedican a los ataques, extorsión y el fraude a través de Internet, en otros, a facilitar el narcotráfico, trata de personas, el comercio y distribución de pornografía infantil, entre otros.

Es decir, las organizaciones cibercriminales funcionan como empresas, contando con expertos especializados para cada tipo de trabajo y ocupación. Entre las especializaciones más comunes que tipifica el FBI son las siguientes:

- ***Programadores:*** *Desarrollan los exploits y el malware que se utiliza para cometer los cibercrímenes.*
- ***Distribuidores:*** *Recopilan y venden los datos robados, actuando como intermediarios.*
- ***Técnicos expertos:*** *Mantienen la infraestructura de la "compañía" criminal, incluyendo servidores, tecnologías de cifrado, bases de datos, etc.*
- ***Hackers[3]:*** *Buscan aplicaciones exploits y vulnerabilidades en sistemas y redes.*
- ***Defraudadores:*** *Crean técnicas de ingeniería social y despliegan diferentes ataques de phishing o spam, entre otros.*
- ***Proveedores de hosting:*** *Ofrecen un entorno seguro para alojar contenido ilícito en servidores y páginas.*
- ***Vendedores:*** *Controlan las cuentas y los nombres de las víctimas y las proveen a otros criminales mediante un pago.*
- ***Muleros:*** *Realizan las transferencias bancarias entre cuentas de banco.*
- ***Blanqueadores:*** *Se ocupan de blanquear los beneficios.*
- ***Líderes de la organización:*** *Frecuentemente, personas normales sin conocimientos técnicos que crean el equipo y definen los objetivos.*

Como asegura dicho informe, las organizaciones cibercriminales se organizan de forma jerárquica, y cada fase diferente de la cadena cuenta con más de un especialista.

Como puede observarse, existen distintos niveles o grados de profesionalización entre los delincuentes (como en muchos otros delitos) en materia de delitos informáticos. Como ya hemos mencionado con anterioridad, suele pensarse que los ciberdelincuentes actúan de forma aislada, espontánea, independiente, de acuerdo a distintas motivaciones. Sin embargo, el transcurso del tiempo y la experiencia en los delincuentes trae consigo la existencia de redes organizadas dedicadas a la comisión de delitos cada vez más complejos, teniendo como consecuencia el aumento de los desafíos a la hora de la investigación por parte de las fuerzas de seguridad, algunos de los cuales veremos más adelante.

Sobre estas bandas organizadas y relacionadas con el delito de la comercialización de pornografía infantil a través de medios informáticos, se pueden citar en Argentina distintos casos de desbaratamientos de complejas redes. Este año por ejemplo, a través de la denominada "Operación Oliver" [2], nacida bajo una investigación previa realizada por las

3 A criterio de estos autores, un "hacker" no es un delincuente, sino un experto de una determinada materia, que con sus conocimientos disfruta de la realización de distintos desafíos intelectuales. Para nosotros, el hecho de ser considerado "hacker" implica de por sí la existencia de una ética propia, que evitaría que se encontrara asociado a una banda organizada de delincuentes como figura en esta categorización citada.

fuerzas de seguridad de Londres, quienes comunicaron a los organismos competentes en Argentina los datos para llevar a cabo una investigación a nivel nacional. A través de la misma, se realizaron 11 allanamientos en la ciudad de Buenos Aires, 24 en el conurbano bonaerense y 26 en distintas provincias (Salta, Tierra del Fuego, San Juan, Tucumán, Santa Fe, Santa Cruz, Córdoba, Santiago del Estero, Chaco, Entre Ríos y Neuquén), con la imputación de 64 personas involucradas.

Deep web y Anonimato

Desde la seguridad de la información, siempre se han tenido ciertas precauciones para hablar o escribir sobre Deep Web, básicamente porque mucha de la información circulante sobre el tema no está verificada ni puede ser adecuadamente chequeada, al menos no con la rigurosidad académica que se necesita hacerlo para este tipo de artículos.

En Internet se pueden encontrar una importante cantidad de artículos, publicados en diversos medios, algunos incluso diarios de importantes nombres, donde se brindan estadísticas sobre la cantidad de contenidos y se afirman determinados datos que no poseen ningún tipo de fuente, o al menos, si las supuestas fuentes existen, la información no se encuentra adecuadamente fundada.

No obstante, la *Deep Web* es un espacio virtual más que existe en la actualidad, cada vez más accesible para los usuarios, y que posee determinadas características que es necesario considerar si se quiere hacer un estudio completo sobre los delitos informáticos.

Esta *Deep web*, o Internet profunda, o Internet oculta no es más que una parte de la red de Internet en la cual los contenidos no son indexados por los motores de búsquedas tradicionales (Google, Yahoo, etc.). Por ello y en contraste con la Deep Web, Internet como la conocemos se la conoce también como Internet superficial.

Los contenidos pueden no ser indexados por ejemplo porque son páginas web dinámicas, sitios bloqueados (por un CAPTCHA por ejemplo), sitios sin linkear, sitios privados (acceso sólo con credenciales de usuario), sitios con contenidos que no son HTML o contextual, así como redes de accesos limitados (por ejemplo, a determinados protocolos de accesos).

Dentro de estos últimos, de contenidos que sólo son accesibles a través de un determinado software o protocolo específico, podemos encontrar al Proyecto TOR, uno de las herramientas más conocidas y de la cual dedicaremos unas líneas a continuación.

TOR [3] fue creado en 2003 por Roger Dingledine, Nick Mathewson y Paul Syverson surgió como la evolución del proyecto Onion Routing del Laboratorio de Investigación Naval de los Estados Unidos. A finales de 2004 pasó a ser patrocinado por la Electronic Frontier Foundation, la organización de defensa de libertades civiles en el mundo digital, hasta noviembre de 2005. Actualmente el proyecto Tor está en manos del 'Tor project' una organización sin ánimo de lucro orientada a la investigación y la educación, radicada en Massachusetts y que ha sido financiada por distintas organizaciones.

Es un proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet, en la que el encaminamiento de los mensajes intercambiados entre los usuarios no revela la identidad de la conexión (dirección IP) permitiendo un anonimato a nivel de red y que, además, mantiene la integridad y el secreto de la información que viaja por ella.

Para la consecución de estos objetivos se ha desarrollado un software libre específico, donde propone el uso de una ruta de conexión del tipo “cebolla”, es decir donde los mensajes viajen desde el origen al destino saltando a través de distintos routers ubicados en distintos puntos del mundo, generando un sistema de protección de la identidad de varias capas (de allí surge el nombre de cebolla).

No desarrollaremos aquí la historia de este proyecto, ni tampoco una descripción técnica detallada sobre el tipo de enrutamiento que propone, toda vez que ello no hace al objetivo en sí del artículo, por lo que nos limitaremos a exponer que el software de cliente Tor construye un circuito de conexiones cifradas a través de repetidores en la red, donde el circuito se extiende un salto a la vez, y cada nodo a lo largo del camino conoce únicamente el nodo que le proporciona los datos y retransmitir los cuales se los entrega. De esta forma, un nodo de forma individual nunca conoce el recorrido completo que ha tomado un paquete de datos. El cliente negocia un paquete separado de claves de cifrado para cada tramo a lo largo del circuito, asegurando la información circulante entre los nodos no pueda ser rastreada. Este circuito de conexión a través de tres nodos distintos, cambia cada aproximadamente diez minutos, dificultando aún más cualquier intento de análisis o *trackeo* de las conexiones circulantes por los nodos.

Nos parece importante destacar que la tecnología explicada de Tor en realidad está enfocada en la protección de los datos en circulación (por eso el sistema de nodos cebolla y el cifrado) pero no en el anonimato en sí. Para eso, los desarrolladores del proyecto lo han completado a través de la generación de un "Tor Browser", un navegador especialmente pensado en la protección de la privacidad del usuario.

Privacidad y anonimato

Conocemos que cada click en un aviso, cada búsqueda realizada, cada página visitada, cada "*Me gusta*", son registrados por algún sistema y forman parte del gran circuito comercial que son la razón de la economía por publicidad en Internet. Desde esta óptica han sido pensados estos proyectos como TOR, buscando brindar a los usuarios herramientas tecnológicas que sirvan como protección frente a tantos avances sobre la privacidad.

La posibilidad de anonimato que brindan estas tecnologías, permite que muchas personas que por distintos motivos (políticos, religiosos, profesionales, etc.) se encuentren bajo distintos niveles de censura y persecución, puedan encontrar un espacio seguro que les permite publicar información, compartir, debatir, donde se encuentre garantizado el derecho a la libertad de expresión en la red.

Por ello, a diferencia de lo que se pretende difundir en diversas notas y medios de comunicación con respecto a TOR y la *Deep Web,* donde se pretende dar una apariencia donde todo lo que existe es pornografía infantil, contenidos gore, venta de drogas y armas, contratación de sicarios, lo cierto es que dentro de esta red oculta encontraremos muchos periodísticas, políticos, profesionales de distintas organizaciones y países que deciden utilizar este espacio para comunicarse y compartir información asegurando su privacidad. También encontraremos personas que quieren hablar sobre conspiraciones, vida extraterrestre y otra gran gama de tópicos, sin temor a ser perseguidos o acusados de forma alguna por la sociedad.

Volviendo a la tecnología en sí, como afirmamos al comienzo de uno de los capítulos, debemos destacar su neutralidad, dejando en claro que la misma fue diseñada y desarrollada con fines más que loables, como el mejoramiento de la privacidad de los usuarios de Internet.

Sin embargo, también es necesario comprender y poner sobre la mesa de debate que esta herramienta que brinda una tecnología con un alto nivel de anonimato, en manos de personas que en vez de buscar asegurar su derecho a la libertad de expresión, buscan un espacio donde se puedan cometer todo tipo de delitos en línea, en forma masiva y con impunidad en la práctica asegurada, representa un problema (y un desafío) para la sociedad y para el Estado.

Desde lo jurídico y como sucede históricamente en el universo jurídico, no existen derechos absolutos, sino limitados precisamente por otros derechos. En este sentido, la propia Convención Americana de Derechos Humanos, si bien prohíbe explícitamente la censura

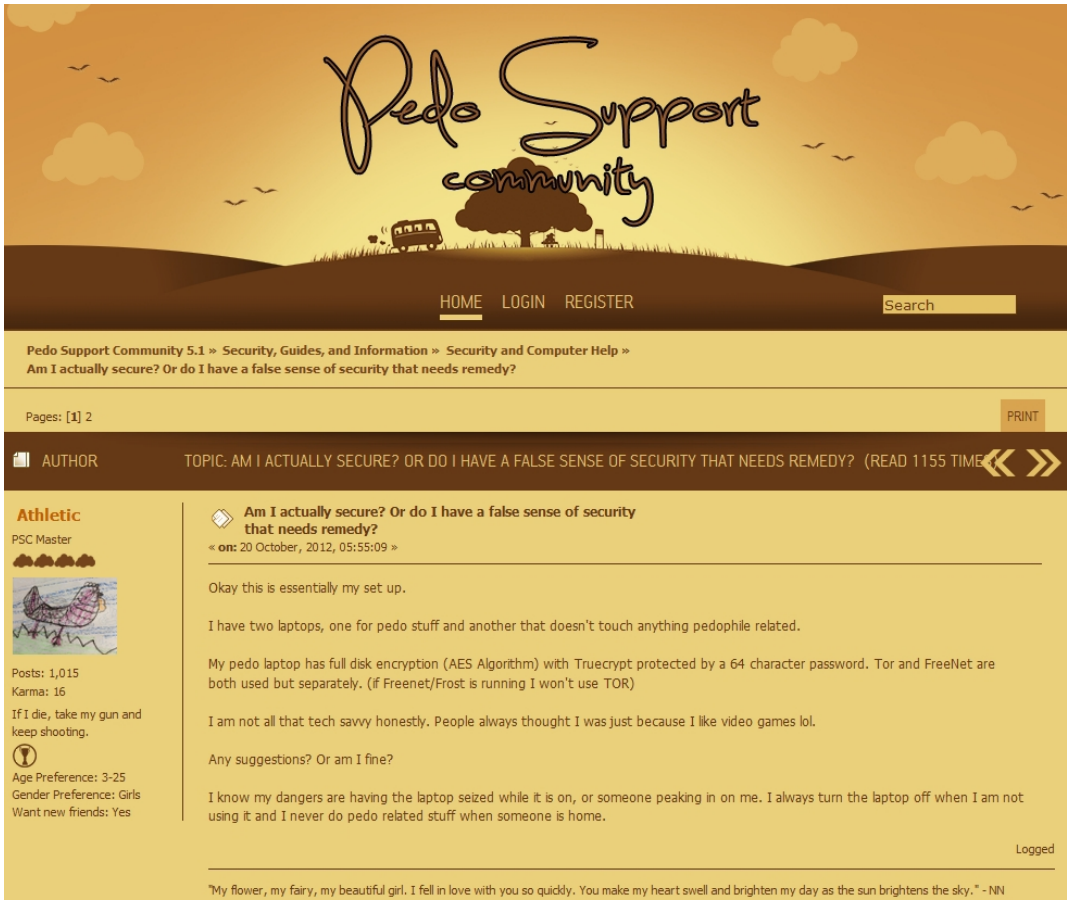
previa, prevee que, bajo ciertas circunstancias, el ejercicio del derecho a la libertad de expresión esté sujeto a responsabilidades ulteriores. Las mismas, "*deben estar expresamente fijadas por ley como para asegurar: a. el respeto a los derechos o a la reputación de los demás, y b. la protección de la seguridad nacional, el orden público o la salud o la moral públicas*". [4]

Nuevamente, sumergirnos en un desarrollo serio sobre las dimensiones de estos derechos, excede la finalidad de este artículo, además que de ya existe doctrina autorizada con extensos trabajos sobre la materia. A los fines de los objetivos planteados sobre la propuesta de una nueva herramienta para la obtención de elementos de prueba, dicha discusión es útil toda vez que es precisamente a través de la utilización de tecnologías que permiten el anonimato, donde comenzamos a encontrar que los delincuentes aprovechan de estos recursos para llevar a cabo la comisión de distintos tipos de delitos, y donde las fuerzas de seguridad se encuentran sin las herramientas adecuadas para llevar adelante investigaciones que tengan buenos niveles de eficacia.

El desafío en la investigación de los delitos informáticos

Al comenzar este artículo ya hemos adelantado que muchos son los desafíos que nos encontramos al investigar delitos donde interviene la tecnología, los que a su vez podríamos categorizarlos en desafíos del tipo técnico, jurídicos y humanos.

Con relación al primer grupo de los desafíos técnicos, nos encontramos con que los delincuentes se encuentran cada día más informados tanto sobre técnicas "antirastreos" como "antiforenses", complejizando o dificultando la labor de los investigadores. A continuación dejamos unos ejemplos extraídos de un foro de soporte para pedófilos:



Pedo_Otaku
Permanently Banned!
Community Hero
Posts: 382
Karma: 0
So long - and thanks for all the paranoia!
Age Preference: 5-12+
Gender Preference: Boys & Girls
Want new friends: No

Re: Am I actually secure? Or do I have a false sense of security that needs remedy?
« Reply #7 on: 15 December, 2012, 07:50:46 »

Quote from: Athletic on 22 October, 2012, 05:52:18

I read about tails but I felt I wouldn't do it right and it would just mess up or some shit. I might eventually but for now I just have fail windows. I might also get a secure linux OS but who knows.

I think I will stick to WiFi... not really worried about that. I don't have bluetooth on.

I have windows update but it is set to not update without my permission.

Another question: Is it okay that I went on TOR while it was encrypting?

You sound pretty secure, but might I suggest routing your TOR traffic through at least another proxy inside a Virtual Machine.

Will a VPN+ VM Hide My IP address
http://m3hjrfh4hlqc67gb.onion/forum/thread/718

I connect to these .onion pedo sites with at least one extra proxy on top of my Tor connection just to be safe.

Using a public unsecured Wifi or your neighbor's hacked WEP Wifi isn't a bad idea either, but make sure you don't use their connection so much that they become suspicious of you. Or better yet, hack into other people's computers and use them as your proxies in a Botnet network. Go for the first option. The second one is not very feasible unless you are uber computer saavy and uber paranoid, but I think some us would want to do that if we could.

Logged

I love kids, but I don't molest them because I am a pedophile and NOT a child molester.

Como se puede observar, es la existencia de un sub foro especial dedicada a técnicas de seguridad de la información, donde se pueden leer consejos y recomendaciones para evitar ser identificados.

A modo genérico diremos que las técnicas antirastreos son todas aquellas que se utilizan con la finalidad de evitar dejar rastros de las acciones realizadas por los delincuentes, imposibilitando o al menos dificultando el "trackeo" por parte de las fuerzas de seguridad. En cambio, las técnicas antiforenses, buscan que ante el caso que las fuerzas de seguridad obtuvieran los dispositivos (notebooks, celulares, discos rígidos, pen drives, etc.), la información que se encuentra en ellos no puedan ser accedidas o analizadas en el marco de una pericia informática, por ejemplo por contar con procesos como cifrado o de borrado seguro (Wiping).

En uno de estos casos, donde los delincuentes utilizan técnicas antirastreo, consideramos que sería uno de los casos donde sería necesaria la incorporación de la figura del agente encubierto digital, a fin de poder obtener información sobre el delincuente, que permitan en el marco de una causa judicial, poder identificarlo y posteriormente, aprehenderlo.

Párrafo aparte también podemos mencionar una lista de situaciones con las cuáles nos podemos encontrar en la práctica de este tipo de investigaciones digitales, donde aquí podemos dividir a los que se conectan desde sus IP "hogareños" (conexión directa), y los que toman algún recaudo para enmascarar o ocultar sus verdaderos direcciones IPs. En referencia al primer grupo de las conexiones directas, podemos encontrarnos con los siguientes situaciones,

- A.1) El Proveedor de Internet (ISP en adelante) colabora y brinda la información para identificar al cliente que realizó la conexión sospechosa.
- A.2) El ISP brinda su colaboración, pero el IP es perteneciente a una subred interna, de la cual no tiene registros de los usuarios que la tenían asignada en un momento dado. (imposibilidad de identificación)
- A.3) El ISP no tiene registro de a qué usuario asigno un IP en un momento dado por Fecha y Hora (hh:mm:ss). (imposibilidad de identificación)
- A.4) El ISP no colabora, argumentando que no tiene una obligación legal de guardar la información de tráfico (imposibilidad de identificación)

En relación al punto A.1 podemos citar que al momento de la redacción del presente artículo, un triste caso conmueve la sociedad argentina. Se trata del caso de Micaela Aldana Ortega, una nena de 12 años captada por *grooming*[4] por un pedófilo que la asesinó en Bahía Blanca[5]. En este caso el presunto asesino de 24 años tenía varias cuentas falsas de Facebook desde donde contactaba a sus posibles víctimas. Tenía cuatro perfiles en Facebook, y un total de 1.700 contactos de los cuales el 90 por ciento eran nenas de la edad de Micaela. En algunos usaba su verdadera identidad y se mostraba ansioso por relacionarse. En otros, como el que usó con la víctima, se hacía pasar por una chica[6]. Como se comentó anteriormente en este trabajo en relación a los factores de dificultad en la investigación de los delitos ocurridos a través de las TICs, tienen especial incidencia en el caso de la actividad de pedófilos y pederastas, a los que Internet posibilita acercarse a sus víctimas aprovechando el alto grado de anonimato y sin despertar sospechas en ellas mediante la utilización de perfiles falsos en las redes sociales más populares entre los menores.

En relación al punto A.2 y A.4, dichos casos son posibles toda vez que en Argentina no existe una legislación que obligue a los proveedores de internet (ISP) a guardar los datos de tráfico de las conexiones, así como tampoco se encuentran reguladas las condiciones sobre las cuáles se puede ofrecer el servicio de Internet, permitiendo que varias empresas (en algunos lugares lo realizan cooperativas) ofrezcan y distribuyan el servicio de Internet utilizando el protocolo NAT[7], que en definitiva permite generar una red interna en la cuál todos los usuarios conectados se conectan a Internet utilizando la misma dirección IP pública.

A criterio de estos autores, es necesario avanzar con una regulación en Argentina que establezca la obligación de retención de los datos de tráfico por parte de los ISP, por un plazo razonable (2 años sería suficiente). Con respecto a este debatido tema, Leopoldo Sebastián Gómez [5] considera que en nuestro país el fallo "Halabi"[8] que declaró inconstitucional la Ley 25.873, Dec. 165/04, y como efecto colateral puede crear un vacío en materia probatorio para ilícitos con tecnología informática, ya que si los proveedores de Internet -o de servicios de telefonía- no están obligados a conservar datos de tráfico será imposible obtener pruebas digitales. Gómez sostiene que es de vital importancia que los legisladores aprueben una ley más completa como la sancionada en España recientemente llamada ley 25/2007 sobre conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, o bien en una normativa como la que se encuentra en la Convención del Cibercrimen, de modo de poder permitir obtener pruebas relacionadas a los delitos informáticos y que ello se realice en colaboración con las empresas proveedoras de telefonía y los ISPs.

---

4 Grooming implica una serie de conductas y acciones deliberadamente emprendidas por un adulto contra un menor, comenzando con una etapa de conexión emocional (confianza), siguiendo con el intercambio de contenidos sexuales (fotos, videos), para posteriormente concluir en la extorsión, amenaza y en el peor de los casos el abuso sexual del menor. En Argentina, dicha conducta fue tipificada por la Ley 26.904, la cuál incorporó el art. 131 al Código Penal.

5 Diario UNO, "Denunciaron más de 200 causas penales por hechos de grooming", Url: http://www.diariouno.com.ar/policiales/denunciaron-mas-200-causas-penales-hechos-grooming-20160531-n797034; Consultado: 01/06/2016

6 Todo Noticias, "El acusado de matar a Micaela siguió buscando víctimas después del crimen", http://tn.com.ar/policiales/el-acusado-de-matar-micaela-siguio-buscando-victimas-despues-del-crimen_677118, Consultado: 01/06/2016

7 NAT (del inglés Network Address Translation) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

8 CSJN, "Halabi, Ernesto c/PEN – ley 25,873- dec. 1563/04 s/amparo ley 16,986", 24/2/2009.

Retomando los posibles obstáculos al momento de una investigación judicial sobre delitos informáticos, en relación a aquellos usuarios que no realizan conexiones directas, nos podemos encontrar con las siguientes situaciones:

- B.1) El ISP colabora, pero el IP corresponde a una organización (pública o privada) que no lleva un control de los IP que asigna. (por ejemplo una Universidad Pública)
- B.2) El ISP colabora, pero el IP corresponde a un Wifi sin contraseña (abierto), y el router no posee habilitado un registro de los IP asignados a los distintos dispositivos.
- B.3) El IP corresponde a una conexión móvil (conexión 3G o 4G desde un Chip), y la empresa telefónica no posee registros de asignación de sus usuarios
- B.4) El IP corresponde a un ISP del extranjero (por ejemplo porque la conexión viene a través de un proxy -VPN, TOR, entre otros-), por lo que será necesaria contar con la cooperación internacional y entender la regulación interna de cada país.

Con respecto al punto B.3 y para añadir información al respecto de las comunicaciones celulares, hoy en día en la Argentina (Mayo 2016) también nos encontramos con la problemática de los "chips prepagos de celulares" que pueden ser adquiridos en cualquier comercio sin acreditar la identidad del comprador. Esto trae aparejado una complejidad anexa, ya que permite a los delincuentes poder realizar llamadas, enviar SMS y conectarse a internet desde el dispositivo celular, o compartiendo internet a otro dispositivo través de un anclaje. Entre las posibilidades de investigación para esta problemática tenemos la vinculación entre el chip, el IMSI[9] y el IMEI[10], el cruzamiento de llamadas y SMS y la localización a partir de las celdas de telefonía pero que necesitan de herramientas específicas para el análisis de los datos, de la colaboración por parte de las telefónica y plantean también el desafío de un modelo unificado de la información que brindan para que sirvan de entradas de las herramientas de análisis.

En relación al punto B.4, el hecho de detectar que la conexión del delincuente se realiza desde lugares remotos del mundo, es un posible indicio de encontrarnos con una las investigaciones más difíciles de llevar a cabo. Como lo hemos desarrollado en el capítulo anterior, nos referimos a aquellas bandas de ciberdelincuentes que utilizan herramientas tecnologícas que brindan grandes niveles de anonimato, usando conexiones a través de TOR y generación de espacios de intercambios en la deep web.

Estos casos suelen ser los de mayor dificultad de investigación para las fuerzas de seguridad, toda vez que las conexiones suelen cambiar cada pocos minutos, conectándose desde distintos proxys anónimos ubicados en distintos lugares del mundo, de difícil cooperación judicial (y aunque existiera, de dudosa utilidad a los fines de la identificación del delincuente). Particularmente en estos casos, es donde se justificaría la utilización de la figura del agente encubierto digital, toda vez que a través de la misma sería posible que los investigadores ingresaran dentro del ámbito de confianza de las bandas de ciberdelincuentes, pudiendo obtener información útil para identificar a los delincuentes por un lado, y para probar los delitos cometidos por otro.

En relación a este mismo desafío de las conexiones internacionales, como autores aprovechamos la oportunidad desde este artículo para expresar la necesidad de adhesión de Argentina al Convenio de Cibercrimen de Budapest, a fin de adecuar la normativa procesal penal por un lado, generándose un Centro de Atención 24/7 para este tipo de investigaciones, y para pertenecer a una red de colaboración internacional para este tipo de casos.

9 IMSI es el acrónimo de International Mobile Subscriber Identity (Identidad Internacional del Abonado a un Móvil). Es un código de identificación único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS.

10 El IMEI (del inglés International Mobile Station Equipment Identity, identidad internacional de equipo móvil) es un código USSD pregrabado en los teléfonos móviles GSM. Este código identifica al aparato de forma exclusiva a nivel mundial, y es transmitido por el aparato a la red al conectarse a esta.

A modo de cierre de este título y volviendo a los desafíos en materia de investigación de la ciberdelincuencia, nos parece adecuado citar a la autora María Victoria Rodríguez Caro [6], quien en un interesante artículo sobre la necesidad del Agente Encubierto Informático, realiza una interesante descripción de los factores que propician la proliferación del crimen informático:

- Por su carácter impersonal, proporciona el anonimato que persigue quien no quiere ser descubierto en sus acciones ilícitas, las cuales a su vez, resultan más fácilmente ejecutables porque crean una mayor conciencia de impunidad (los delitos de injurias, calumnias, contra la integridad moral, incluso en ámbitos como la violencia de género o escolar, tienen un caldo de cultivo gracias a las redes sociales).
- La incomparable capacidad de difusión que proporciona, constituyendo una herramienta inigualable para la perpetración de determinados delitos y la consecución de los fines perseguidos por sus autores (destaca el terrorismo).
- A su vez, Internet es una fuente inabarcable de información que el ciberdelincuente a la vez extrae y emplea, dotando de nueva dimensión a delitos tan clásicos como la estafa, pero logrando mayores dificultades de persecución y control policial.
- En especial, el desarrollo del comercio electrónico en las últimas décadas ha venido acompañado del avance de la delincuencia que aprovecha las oportunidades que proporcionan los puntos débiles del sistema para obtener un lucro ilícito.
- La facilidad de obtención y difusión de contenidos multimedia favorece los comportamientos delictivos que recaen sobre este tipo de soporte, como ocurre con el incremento exponencial de ataques de todo tipo contra los derechos de propiedad intelectual.
- El carácter global del sistema y la falta de fronteras, naturales o políticas, unido a la inmediatez de la transmisión de la información favorece la difusión y perpetración de los delitos y contribuye a universalizar determinadas formas de delincuencia.

Agente encubierto y Agente provocador

Con el paso del tiempo la doctrina ha ensayado distintos conceptos sobre el agente encubierto, enfatizando las diferencias con respecto a la figura del agente provocador.

De acuerdo a Angel Rendo[11], el agente encubierto es "*un empleado o funcionario público que voluntariamente, y por decisión de una autoridad judicial, se infiltra en una organización delictiva a fin de obtener información sobre la misma en relación a sus integrantes, funcionamiento, financiación*".

Néstor Sagues[12] afirma claramente la distinción entre esta figura y el agente provocador que aparece cuando el agente encubierto se involucra de tal manera que hubiese creado o instigado la ofensa criminal en la cabeza del delincuente, y que ha sido recogida por la jurisprudencia argentina.

Otro autor como Fabricio Guariglia[13], expresa que el agente encubierto es "*el miembro de las fuerzas policiales que, ocultando su verdadera identidad, busca infiltrarse en*

11 RENDO, Angel Daniel."Agente Encubierto" en http://www.abogarte.com.ar/agenteencubierto.htm

12 SAGUES, Pedro Néstor."Libertad personal, seguridad individual y debido proceso en Argentina" en Ius et Praxis, Talca, Chile, 1999, Nº1, pp. 225 - 226.

13 GUARIGLIA, Francisco."El agente encubierto ¿un nuevo protagonista en el procedimiento penal? En http://www.cienciaspenales.org/REVISTA%2012/guarig12.htm

organizaciones delictivas con el fin de recabar información". Además sostiene que esta figura que se introduce en el esquema clásico del procedimiento penal es un nuevo método a utilizar por la reacción penal estatal.

Un punto de vista más restringido pero no por eso menos importante, es el José Cafferatas Nores[14], quien sostiene que el agente encubierto junto con otras técnicas de investigación constituyen medios de prueba extraordinarios, que si bien se utilizan en un principio para enfrentar serios problemas a su vez extraordinarios, encierran el grave riesgo de legitimar la ilegalidad en la investigación penal. Según este autor existe en la actualidad una tendencia a que estos medios de prueba extraordinarios se ordinaricen. Señala además que "*el agente encubierto es un funcionario público que fingiendo no serlo, se infiltra por disposición judicial en una organización delictiva con el propósito de proporcionar desde adentro, información que permita el enjuiciamiento de sus integrantes, y como consecuencia, el desbaratamiento de esa asociación ilícita; el agente encubierto es aquel funcionario público que simula ser delincuente*". Por último, Cafferatas, señala que el agente encubierto para que pueda utilizarse en un caso concreto debe cumplir con ciertas condiciones. Estas condiciones son: excepcionalidad, taxatividad y sanciones:

- **Excepcionalidad:** Esto se relaciona con el principio de subsidiariedad en el sentido de que la utilización del agente encubierto se reserva cuando el esclarecimiento de los hechos no es posible lograrlo por vías ordinarias.
- **Taxatividad:** Sólo debe utilizarse en procesos y delitos que taxativamente se autoricen, excluyéndose la posibilidad de que se introduzcan en investigaciones que no tenga carácter penal.
- **Sanciones:** El establecimiento de sanciones penales especiales para el agente encubierto que proporcione datos inexactos o formule imputaciones falsas.

De acuerdo a Mario Montoya[15] la diferencia entre el agente encubierto y el provocador radica en que este último hace cometer un delito a quien no lo hubiera hecho, a no ser por el engaño, mientras que el agente encubierto en cambio "*se infiltra entre quienes están cometiendo delitos, con el fin de proporcionar informaciones que obtiene de los investigados, y que prueba la anterior y libre disposición del sujeto para cometer delitos*".

Muñoz Pope[16] nos enseña que el agente provocador es aquel sujeto que induce a otro a cometer un delito para que en el intento de realizar el mismo se le detenga y, eventualmente, se le declare penalmente responsable por la conducta realizada, pues el actuar provocado supone por lo menos un inicio en la ejecución del delito que ha puesto en peligro el bien jurídico que aquel, es decir, el agente provocador tiene interés en preservar. No puede confundirse, por otra parte, el agente provocador con el llamado agente encubierto, ya que este último es "*un agente policial que sólo limita su actuación a conocer el contexto real en una determinada investigación criminal y recabar la prueba necesaria para enjuiciar y eventualmente condenar al infractor de la ley penal"*.

A modo de resumen o extracto general de todos los autores consultados, observamos entonces que la diferencia entre ambas figuras es que el agente encubierto no está provocando la consumación del delito, ni induce a la conducta ilícita, sino que lo que hace es agregar un eslabón probatorio más dentro del marco de una causa judicialmente controlada. En cambio, el agente provocador tiende a inducir a la consumación del delito, con el claro riesgo de afectación a derechos y garantías constitucionales, toda vez que el sujeto provocado actúa sin libertad ni espontaneidad ya que el delito surge por la maquinación del agente provocador.

---

14 CAFERATTA NORES, José ."Cuestiones actuales sobre el proceso penal". Editores del Puerto, Buenos Aires 2000, pp. 221 - 231

15 MONTOYA, Mario Daniel " "Informantes y técnicas de investigación encubierta" de Mario Daniel Montoya. Ad Hoc. 2001.

16 MUÑOZ POPE, Carlos "Ensayos penales. El agente provocador". Ed. Panamá Viejo, Panamá, 2001.

Precisamente entre las críticas hacia el agente provocador, se sostiene que el agente a través de un engaño induce al sujeto provocado a cometer un delito que de otro modo no se hubiese cometido. Por tal motivo, consideramos que en el marco del planteo de la necesidad de incorporación de la figura del agente encubierto digital, es importante delimitar bien las facultades y restricciones de la figura, ya que como sostuvo el Tribunal Europeo de Derechos Humanos en relación a una causa donde se había puesto en discusión su legitimidad, se sostuvo que "*el uso de agentes encubiertos debe evitar, traspasar los límites de su trabajo de investigación y convertirse en provocador*"[17]

Con respecto a estos límites y garantías, nuestra Corte Suprema de Justicia de la Nación también ha tenido ya oportunidad de expedirse en un *leading case* sobre la utilización del agente encubierto tradicional, en el marco de una causa de narcotráfico, como ha sido el caso "Fiscal c/ Fernández"[18]. En el caso, se ha dejado constancia que "*es criterio de esta Corte que el empleo de un agente encubierto para la averiguación de los delitos no es por si mismo contrario a garantías constitucionales. Una cuidadosa comprensión de la realidad de nuestra vida social común, y en especial el hecho comprobado de que ciertos delitos de gravedad se preparan e incluso ejecutan en la esfera de intimidad de los involucrados en ellos, como sucede particularmente con el tráfico de estupefacientes, impone reconocer que esos delitos sólo son susceptibles de ser descubiertos y probados si los órganos encargados de la prevención logran ser admitidos en el círculo de intimidad en el que ellos tienen lugar. Por tal razón, una interpretación prudencial de las garantías procesales contenidas en la Constitución Nacional permite aceptar, bajo ciertas restricciones, el empleo de agentes encubiertos de modo similar al que se lo admite en otros países en los que las reglas del Estado de Derecho proscriben garantías análogas a las que rigen en la República Argentina; entre los cuales cabe citar a los Estados Unidos (confr. "Lewis v. U.S.. 385 US 206) y a la República Federal de Alemania (confr. BGH Gr. S. St. 32, 115, 122: BverfGE 57.250, 284, y la decisión del GBH en NStZ. 1982, 40)*."

En el considerando siguiente, la Corte ha dicho que "l*a conformidad en el orden jurídico del empleo de agentes encubiertos requiere que el comportamiento de ese agente se mantenga dentro de los principios del Estado de Derecho (así lo sostuvo en Alemania el BGH, confr. decisión en NStZ 1984, 78), lo que no sucede cuando el agente encubierto se involucra de tal manera que hubiese creado o instigado la ofensa criminal en la cabeza del delincuente, pues la función de quienes ejecutan la ley es la prevención del crimen y la aprehensión de los criminales, pero esa función no incluye la de producir el crimen tentando a personas inocentes a cometer esas violaciones (confr. "Sorreis v. U.S.". 287 US 435). De tal modo, cabe distinguir los casos en que los agentes del gobierno simplemente aprovechan las oportunidades o facilidades que otorga el acusado predispuesto a cometer el delito, de los que son "producto de la actividad creativa" de los oficiales que ejecutan la ley (confr. además del caso citado de 287 US 435, "Sherman v. U.S. ", 356 US 369 y "Hampton v. U.S.". 425 US 484) en los que procede desechar las pruebas obtenidas por la actividad "criminógena" de la policía bajo lo que en el derecho americano se conoce como defensa de entrapment (confr. "Woo Wai v. U.S.". 223 US 412 y "U.S. v. Russell". 411 US 423, además del ya citado caso de 287 US 435).*"

A modo de conclusión de este título y retomando lo sostenido por nuestra Corte Suprema de Justicia de la Nación, se reconoce que bajo ciertas condiciones y para determinados delitos, la figura del agente encubierto puede utilizarse en nuestro sistema, y que la misma de por sí no es violatorio de garantías constitucionales.

---

17 Tribunal Europeo de Derechos Humanos. Causa: Texeira de Castro vs Portugal, Judgement 9/6/1998-Report of Judgment and Decisions-1998/IV-1464.

18 'Fiscal c/ Fernández, Víctor Hugo s/ av. infracción ley 20.771' - CSJN - 11/12/1990

Legislación vigente

En Argentina existe regulación sobre el agente encubierto, pero solamente autorizado en determinados delitos. La figura se encuentra regulada dentro de la Ley Nro. 23.737, conocida como la “Ley de estupefacientes”, sancionada en el año 1989. La citada ley originalmente no había regulado la figura del agente encubierto, sino que la misma fue agregada en el año 2005, a través de la Ley N° 24.424, que modificó en varios aspectos a la Ley 23.737, entre ellos el instituto del agente encubierto:

> **ARTICULO 6º — Incorpórase como artículo 31 bis a la ley 23.737, el siguiente:**
> "Artículo 31 bis: Durante el curso de una investigación y a los efectos de comprobar la comisión de algún delito previsto en esta ley o en el artículo 866 del Código Aduanero, de impedir su consumación, de lograr la individualización o detención de los autores, partícipes o encubridores, o para obtener y asegurar los medios de prueba necesarios, el juez por resolución fundada podrá disponer, si las finalidades de la investigación no pudieran ser logradas de otro modo, que agentes de las fuerzas de seguridad en actividad, actuando en forma encubierta:
> a) Se introduzcan como integrantes de organizaciones delictivas que tengan entre sus fines la comisión de los delitos previstos en esta ley o en el artículo 866 del Código Aduanero, y
> b) Participen en la realización de alguno de los hechos previstos en esta ley o en el artículo 866 del Código Aduanero.
> La designación deberá consignar el nombre verdadero del agente y la falsa identidad con la que actuará en el caso, y será reservada fuera de las actuaciones y con la debida seguridad.
> La información que el agente encubierto vaya logrando, será puesta de inmediato en conocimiento del juez.
> La designación de un agente encubierto deberá mantenerse en estricto secreto. Cuando fuere absolutamente imprescindible aportar como prueba la información personal del agente encubierto, éste declarará como testigo, sin perjuicio de adoptarse, en su caso, las medidas previstas en el artículo 31 quinques".
>
> **ARTICULO 7º — Incorpórase como artículo 31 ter a la ley 23.737, el siguiente:**
> "Artículo 31 ter: No será punible el agente encubierto que como consecuencia necesaria del desarrollo de la actuación encomendada, se hubiese visto compelido a incurrir en un delito, siempre que éste no implique poner en peligro cierto la vida o la integridad física de una persona o la imposición de un grave sufrimiento físico o moral a otro.
> Cuando el agente encubierto hubiese resultado imputado en un proceso, hará saber confidencialmente su carácter al juez interviniente, quien en forma reservada recabará la pertinente información a la autoridad que corresponda.
> Si el caso correspondiere a las previsiones del primer párrafo de este artículo, el juez lo resolverá sin develar la verdadera identidad del imputado".
>
> **ARTICULO 8º — Incorpórase como artículo 31 quater a la Ley 23.737, el siguiente:**
> "Artículo 31 quater: Ningún agente de las Fuerzas de seguridad podrá ser obligado a actuar como agente encubierto. La negativa a hacerlo no será tenida como antecedente desfavorable para ningún efecto".
>
> **ARTICULO 9º — Incorpórase como artículo 31 quinques a la Ley 23.737, el siguiente:**
> "Artículo 31 quinques: Cuando peligre la seguridad de la persona que haya actuado como agente encubierto por haberse develado su verdadera identidad, tendrá derecho a optar entre permanecer activo o pasar a retiro, cualquiera fuese la cantidad de años de servicio que tuviera. En este último caso se le reconocerá un haber de retiro igual al que le corresponda a quien tenga dos grados más del que él tiene.
> En cuanto fuere compatible, se aplicarán las disposiciones del artículo 33 bis".
>
> **ARTICULO 10. — Incorpórase como artículo 31 sexies a la Ley 23.737, el siguiente:**
> "Artículo 31 sexies: El funcionario o empleado público que indebidamente revelare la real o nueva identidad de un agente encubierto o, en su caso, la nueva identidad o el domicilio de un testigo o imputado protegido, será reprimido con prisión de dos a seis años, multa de diez mil a cien mil pesos e inhabilitación absoluta perpetua.

> El funcionario o empleado público que por imprudencia, negligencia o inobservancia de los deberes a su cargo, permitiere o diere ocasión a que otro conozca dicha información, será sancionado con prisión de uno a cuatro años, multa de un mil a treinta mil pesos e inhabilitación especial de tres a diez años.

Como se puede observar en la legislación citada, la regulación sobre la figura es extensa y detallada, destacándose entre sus requisitos la necesidad de autorización judicial para que la figura del agente encubierto pueda ser puesta en práctica en el marco de una investigación judicial.

No ahondaremos en un análisis jurídico exhaustivo sobre dichos artículos, toda vez que excedería el objeto del presente artículo, pero si es necesario comprender las características del instituto, a fin de determinar si podría llegar a ser posible la ampliación de la figura o bien, si sería la posible la propuesta de la figura del agente encubierto digital, pero en otro cuerpo normativo.

En relación a los sujetos autorizados, de acuerdo al art. 31 bis el agente encubierto debe ser un integrante de las fuerzas de seguridad en actividad. Es decir, que deja fuera de margen la posibilidad que un civil pueda llegar a actuar como agente encubierto, lo cual luce como acertado a la luz que los agentes encubiertos deben poseer una preparación especial para llevar a cabo sus tareas con éxito, más aún cuando, como ya hemos aclarado ut supra, actualmente es una figura que puede utilizarse solamente para casos de crimen organizado o tráfico de estupefacientes. Por otro lado, el hecho que sea un agente de seguridad, permite ejercer el control de una forma más directa por parte de las autoridades competentes.

En relación al alcance o ámbito de aplicación, el mismo art. 31 bis sostiene que "*Durante el curso de una investigación y a los efectos de comprobar la comisión de algún delito previsto en esta ley o en el artículo 866 del Código Aduanero*", afirmando que el agente encubierto sólo podrá ser utilizado durante el curso de una investigación de un delito de narcotráfico o crimen organizado (objeto de dicha ley) o casos del art. 866 del Código Aduanero, y sólo únicamente será dispuesta, dirigida y controlada por el juez federal, cumpliendo estos requisitos:

1) Cuando las finalidades de la investigación no pudieran ser logradas de otro modo (art. 31 bis, 1er. párr.), si el magistrado subsidiariamente aprecia que es necesario el empleo de agentes en actividad de las fuerzas de seguridad para actuar en forma encubierta, deberá hacerlo por resolución fundada bajo pena de nulidad (art. 31 bis, 1er. párr.; CPP, art. 123, 1ra. regla). Dicha fórmula nos parece adecuada, toda vez que como si hace falta una orden judicial para efectuar un allanamiento, es bueno requerir la autorización cuando se trata de este tipo de investigaciones.

2) La designación debe consignar el nombre verdadero del agente y la falsa identidad con la que actuará en el caso, la cual se mantendrá en principio bajo estricto secreto (art. 31 bis, 3er. párr. y 5to. párr., 1ra. Regla).

3) Las actuaciones encubiertas están bajo el directo control judicial, porque la información que el agente infiltrado vaya logrando, será puesta de inmediato en conocimiento del juez (art. 31 bis, 4to.párr.).

Derecho comparado

En Chile, a través de la Ley 19.366 se propuso "*dotar al ordenamiento jurídico de instrumentos que permitan enfrentar con mayor eficacia los problemas derivados del tráfico ilícito y del consumo de drogas estupefacientes, perfeccionando las disposiciones actualmente vigente*" [7]. Posteriormente, dicha norma ha sido modificada por la Ley 20.000, en cuyo artículo 25 de la ley 20.000 señala:

> "El Ministerio Público podrá autorizar a funcionarios policiales para que se desempeñen como agentes encubiertos o agentes reveladores y, a propuesta de dichos funcionarios, para que determinados informantes de esos servicios actúen en alguna de las dos calidades anteriores".
>
> "Agente encubierto es el funcionario policial que oculta su identidad oficial y se involucra o introduce en las organizaciones delictuales o en meras asociaciones o agrupaciones con propósitos delictivos, con el objetivo de identificar a los participantes, reunir información y recoger antecedentes necesarios para la investigación."
>
> "El agente encubierto podrá tener una historia ficticia. La Dirección Nacional del Servicio de Registro Civil e Identificación deberá otorgar los medios necesarios para la oportuna y debida materialización de ésta."

Como podemos observar, a diferencia de Argentina, en Chile el agente encubierto podría desplegar su actividad en casos de terrorismo, crimen organizado y seguridad nacional (ley 19.974) y tráfico de drogas (ley 20.000). Además, por la fórmula utilizada sobre el ámbito de actuación de estas figuras es un poco más amplio, al permitir su utilización en organizaciones delictivas o meras asociaciones o grupos con propósitos delictivos. Siguiendo a Eduardo Riquelme Portilla [8], para esta definición normativa el grupo no necesariamente debe ser una banda de narcotraficantes, sino que basta que sea un grupo de sujetos que se apresten a cometer delitos.

Por otro lado, observamos que en Chile, no sólo se autoriza a funcionarios policiales sino también a civiles informantes de la policía, a propuesta de dichos funcionarios, una solución que como ya expresamos anteriormente, no nos parece del todo adecuada.

En Alemania también existe esta figura desde el año 1992, a través de su regulación legislativa en la Ley para el combate del tráfico ilícito de estupefacientes y otras formas de aparición de la criminalidad organizada (Gesetz zur Bekampfung des illegalen Rauschgifthandels und anderer Eerscheinngformen der Organisierten Kriminalitat-OrKG).

De acuerdo a Felipe Sologuren Insua [9], esta norma alemana define el agente encubierto como aquel miembro del servicio policial que indaga bajo una identidad alterada (legende, "leyenda"), otorgada por un período limitado de tiempo. Esta definición excluye a los miembros de la policía que se hayan infiltrado sólo como producto de la ocasión y también a los hombres-V que son para nosotros los informantes. Esto tiene mucha importancia práctica ya que evidentemente tienen una regulación más intensa en cuanto a los requisitos para poder desarrollar la actividad los agentes encubiertos que los informantes. El problema que se ha suscitado es que los órganos persecutorios podrían evitar las limitaciones que tiene el agente encubierto mediante el empleo de hombres-V (que no son miembros de la policía), en cuanto se podrían saltar las barreras que restringen la utilización de los agentes encubiertos. A esto se ha argumentado que la consecuencia de esta situación sería la imposibilidad de valorar judicialmente la información así obtenida, (por lo hombres-V), en circunstancias de que esta situación no está amparada por la normativa que regula el agente encubierto.

También es importante destacar que la legislación alemana para la creación y mantención de la identidad falsa del agente encubierto, admite la confección, modificación y utilización de los documentos respectivos, cosa que la ley no define, y le ha tocado a la doctrina su delimitación, señalando que los documentos respectivos son aquellos que habitualmente se utilizan para certificar la identidad, sin que sea posible la alteración de libros y registros públicos.

En relación al ámbito de aplicación, el agente encubierto germano aparece justificada en una importante variedad de casos, como delitos de tráfico de estupefacientes; de armas; de falsificación de dineros; ámbito de protección del Estado; crimen organizado; delitos castigados con penas privativa de libertad mínima de un año o superior, siempre que haya peligro de reiteración, entre otros, incrementando notablemente la posibilidad de aplicación de la figura.

Para cerrar con el repaso de otras legislaciones, dejamos para lo último la interesante regulación española sobre esta figura, quien introdujo a través de las últimas modificaciones a la Ley de Enjuiciamiento Criminal[19], nuevas herramientas para la investigación penal, particular la que interesa a los fines de este artículo: el agente encubierto digital. A continuación, dejaremos un extracto del artículo más importante en relación a nuestro objeto de estudio:

> **Artículo 282 bis**
>
> 1. A los fines previstos en el artículo anterior y cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos. La identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico y social bajo tal identidad.
>
> La resolución por la que se acuerde deberá consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto.
>
> La resolución será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad.
>
> La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente.
>
> 2. Los funcionarios de la Policía Judicial que hubieran actuado en una investigación con identidad falsa de conformidad a lo previsto en el apartado 1, podrán mantener dicha identidad cuando testifiquen en el proceso que pudiera derivarse de los hechos en que hubieran intervenido y siempre que así se acuerde mediante resolución judicial motivada, siéndole también de aplicación lo previsto en la Ley Orgánica 19/1994, de 23 de diciembre.
>
> Ningún funcionario de la Policía Judicial podrá ser obligado a actuar como agente encubierto.
>
> 3. Cuando las actuaciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables.
>
> 4. A los efectos señalados en el apartado 1 de este artículo, se considerará como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes:
>
> a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.
>
> b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.
>
> c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.
>
> d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal.
>
> e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.
>
> f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal.
>
> g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal.
>
> h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal.
>
> i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal.
>
> j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal.

19 Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales; Publicado en BOE núm. 239, de 6 de octubre de 2015, páginas 90220 a 90239. Url: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10726, Consultado: 01/06/2016

k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.

l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.

m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal.

n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal.

o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando.

5. El agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito.

Para poder proceder penalmente contra el mismo por las actuaciones realizadas a los fines de la investigación, el Juez competente para conocer la causa deberá, tan pronto tenga conocimiento de la actuación de algún agente encubierto en la misma, requerir informe relativo a tal circunstancia de quien hubiere autorizado la identidad supuesta, en atención al cual resolverá lo que a su criterio proceda.

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.

Son varios los aspectos destacables del presente artículo, pero en honor a la brevedad mencionaremos sólo algunos a fin de mantener la comparación de los otros regímenes legales ya observados.

En relación a los sujetos que pueden ser agentes encubiertos, España ha adoptado una solución donde será el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, los que podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación.

En cuanto al ámbito de aplicación de la figura, en el inciso 4 se destaca una descripción útil a los fines de fijar posiciones jurídicas, afirmando que "*se considerará como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes*". Allí, a través de los sub incisos se describen todos los delitos en lo cuáles podrían aplicarse el agente encubierto, que como se puede observar es la más amplia en comparación a los otros ordenamientos que hemos estudiado.

Por último, y quizás como elemento más importante desde nuestra óptica, observamos que en el inciso 6 existe una regulación especial para permitir la utilización del "*agente encubierto informático*", en el que previa autorización del juez, se podrá utilizar la figura para actuar en "*comunicaciones mantenidas en canales cerrados de comunicación [...]*". A párrafo seguido, se regula la posibilidad de que el agente encubierto informático, previa autorización específica que lo permita, pueda "*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*". Esta opción es muy importante para la finalidad buscada en la figura, toda vez que por ejemplo, en el caso de las redes de distribución de pornografía infantil, para pertenecer a un grupo o foro cerrado dedicado a esa actividad, es

muy posible que sea necesario que el usuario (agente encubierto informático o digital) tenga que intercambiar o enviar al grupo contenidos de este tipo, a fin de ser aceptado por el grupo y generar la confianza necesaria, generando el entorno adecuado para que posteriormente se puedan llevar a cabo las tareas de recolección de información clásicas de un agente encubierto.

Sobre el tema, es interesante lo afirmado en el Boletín del Ministerio de Justicia de España [10], sobre que las Fuerzas y Cuerpos de Seguridad del Estado Español desarrollan habitualmente rastreos o sondeos de contenidos en la Red con fines preventivos o investigativos, afirmando que siempre que estos rastreos se lleven a cabo dentro en la Red pública no requiere ninguna garantía adicional más que su previsión legal, que se viene a considerar comprendida dentro de las facultades propias de estos Cuerpos Policiales (art. 282 LECrim y 11.1 LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad), con el sustento que proporciona el Convenio sobre Cibercrimen de 2001 (art. 32).

El mismo informe, reconoce que un "*avance reseñable de la ley de reforma es la regulación del agente encubierto informático, ampliando el ámbito de actividad de esta figura al mundo digital, cuya eficacia en la persecución de actividades propias de la delincuencia organizada es justo destacar. De acuerdo con las nuevas previsiones el juez podrá autorizar a funcionarios de la Policía para intervenir bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, si bien determinadas actuaciones como el intercambio o envío de archivos ilícitos por razón de su contenido requerirá de una nueva autorización expresa (art. 282 bis 6)*"

Aunque no exista remisión expresa en la ley, se entiende que al agente encubierto informático le será aplicable la previsión relativa a la exclusión de conductas que "*constituyan provocación del delito*", que se predica del infiltrado ordinario (art. 282 bis.5), con las consecuencias contempladas jurisprudencialmente determinantes de la impunidad del comportamiento seguido por el sujeto provocado en caso de incumplimiento, a efectos de que la utilización de dicha figura deviniera en un "agente provocador", con todas las consecuencias jurídicas que ello traería aparejado.

Habida cuenta las ramificaciones internacionales de la delincuencia organizada y la ya mencionada ausencia de fronteras para las comunicaciones digitales es preciso que la adopción de esta clase de medidas de investigación como las del agente encubierto informático, especialmente en cuanto al intercambio de archivos ilícitos, vaya acompañada de la activación de los instrumentos de cooperación policial a nivel internacional, por ejemplo, el Convenio de Cibercrimen de Budapest[20].

El agente encubierto informático o digital

Tomando como punto de partida la regulación española, intentaremos aquí abordar una serie de observaciones por las cuales consideramos como necesaria la regulación en Argentina de la figura del agente encubierto informático o digital.

Para comenzar con la fundamentación, nos parece acertado citar el análisis realizado por María Victoria Rodríguez Caro, Licenciada en Derecho y en Criminología; Máster en Sistema penal, Criminalidad y Políticas de Seguridad, Abogada y Fiscal Sustituta. En un artículo de doctrina publicado por esta autora[21], se realiza un especial comentario en lo que se ha dado en llamar ciberdelincuencia, cuya importancia ascendente motiva la necesidad de reformas o adaptaciones en relación a las herramientas de investigación. En palabras de esta autora, "*Internet constituye un nuevo espacio en el que se desarrolla la actividad delictiva*

20 Convenio de Cibercrimen de Budapest; CETS No. 185, Url: http://www.coe.int/es/web/conventions/full-list/-/conventions/treaty/185

21 op. cita bibliográfica número 6.

más diversa, y la figura del agente encubierto se muestra como un medio eficaz para el descubrimiento y la persecución de quienes se aprovechan de la red para sus propósitos".

Sostiene que los factores que ya se analizaron en cuanto al desarrollo de la ciberdelincuencia, especialmente el anonimato, la falta de contacto directo delincuente-víctima y la prosperabilidad del engaño, son los que "*hacen adecuada la investigación encubierta para el descubrimiento de los responsables de este tipo de delitos, especialmente graves por la vulnerabilidad de los destinatarios del ataque*".

Se hace también un interesante análisis acerca del concepto de organización en la red, a fin de analizar si sería aplicable la figura considerando que estos delitos en internet, podrían llegar a ser considerados como crimen organizado. En este sentido, Rodriguez Cano trabaja que el concepto de organización en la red también presenta perfiles propios, lo que se refleja en la propia posición de la jurisprudencia (española). Conforme a la STS 1444/04, de 10 de diciembre, "*tendrán la consideración de grupos organizados cualesquiera aquellos lugares de encuentro que son utilizados en Internet para la interrelación de diversas personas en torno a un tema común y con la finalidad, en muchos casos, de intercambiar material multimedia referido a ese tema, como serían los chats, comunidades virtuales, redes sociales, blogs, etc*." Por el contrario, la STS 913/2006, de 20 de septiembre, opta por un concepto más restrictivo, para que pudiera hablarse de organización delictiva, sería necesaria una estructura más compleja que la existente en los referidos lugares de encuentro de Internet.

Esta autora realiza aquí un razonamiento en cuanto al nacimiento de la figura del agente encubierto para la investigación del narcotráfico, actividad esencialmente organizada, que dota de una especial gravedad y trascendencia socio-económica al delito de tráfico de drogas, especialmente nocivo cuando penetra en las instituciones del mismo Estado. Y lo que para este caso se preveía como natural, para el resto de los delitos se convierte en un estándar de proporcionalidad. Es decir, es posible la implementación de la investigación encubierta cuando, aun tratándose de la investigación de delitos menos graves se trate de investigaciones que afecten a actividades propias de la delincuencia organizada. La razón de ser radica, de un lado en la especial gravedad de los delitos cometidos por las organizaciones criminales debido a la mayor facilidad para la perpetración por los mecanismos y medios empleados, el incremento de la impunidad que proporciona a los integrantes de la organización, así como de los potenciales efectos del delito; junto a ello, se justifica la necesidad de emplear medios de investigación nuevos para formas nuevas de delincuencia, allí donde fracasan los métodos tradicionales.

La importancia del desarrollo realizado por Rodriguez Cano, tiene como corolario afirmar que todos estos aspectos que son determinantes de la gravedad de las conductas y justifican el empleo de un agente de seguridad infiltrado, concurren en el caso de los delitos cometidos a través de Internet (incremento de la facilidad de perpetración, de la impunidad y de los efectos), en especial la necesidad de emplear métodos nuevos allí donde los tradicionales no alcanzan (máxime cuando se trata de delitos relativos a la prostitución de menores y pornografía infantil). En consecuencia, la conceptuación de la exigencia de que se trate de actividades propias de la delincuencia organizada quizás debería adaptarse a la realidad de los grupos de intercambio de material de pornografía infantil en la red.

Del mismo modo, también el concepto de agente encubierto puede adaptarse en el ámbito de la ciberdelincuencia en general y de la pornografía infantil en Internet en particular, en tanto en cuanto precisamente por el anonimato que proporciona el medio, no se necesita que se proporcione al agente encubierto la completa identidad falsa que es precisa en la compleja operación de infiltración ordinaria, bastando una identidad virtual, como menor o como pedófilo, y en su caso la creación de cuentas de una cuenta de correo electrónico o línea telefónica a fin de habilitar tales cuentas.

Finalmente, esta autora sostiene (adecuadamente desde nuestro criterio), que en cuanto al intercambio de material de pornografía infantil, su uso por parte de las fuerzas de seguridad deberá pasar el filtro de la proporcionalidad, en función de la finalidad perseguida (igual que ocurre con la posesión o el transporte de drogas), de forma que la menor gravedad venga determinada por la índole del material difundido (mayor edad de los afectados, imágenes que no sean especialmente degradantes, y se trate de material ya difundido, procedente de intervenciones anteriores).

En relación a este desarrollo, nos parece oportuno aquí destacar unas líneas sobre la jurisprudencia ya vista de nuestra CSJN, en el caso "Fiscal c/ Fernandez" donde se afirmó que "*el hecho comprobado de que ciertos delitos de gravedad se preparan e incluso ejecutan en la esfera de intimidad de los involucrados en ellos, como sucede particularmente con el tráfico de estupefacientes, impone reconocer que esos delitos sólo son susceptibles de ser descubiertos y probados si los órganos encargados de la prevención logran ser admitidos en el círculo de intimidad en el que ellos tienen lugar*".

Siguiendo esta línea de razonamientos, la CSJN reconoce que la figura del agente encubierto, se encuentra fundamentada en que estamos ante la presencia de delitos graves y cuya ejecución se realiza dentro de un círculo de intimidad, ambos requisitos cumplidos cuando nos enfrentamos a la investigación de delitos cuyo bien jurídico afectado es la integridad de un menor, y donde se utiliza la tecnología como medio de comisión, dotando de complejidad a la detección e identificación de los autores, así como en una adecuada recolección de la evidencia digital.

En este mismo sentido, el autor Hugo Vaninetti [11] sostiene que la figura del agente encubierto para la investigación de los delitos relacionados con la pornografía infantil en internet debe ser legislada y de manera muy estricta. Este autor trabaja un tema interesante en cuanto a la interpretación de la figura del agente encubierto, expresando que las infiltraciones sencillas, que tan sólo afloran la previamente exteriorizada voluntad delictiva de quien ofrece el objeto prohibido (por ejemplo la pornografía infantil), no se pueden confundir con la provocación delictiva, ni precisan de más exteriorizaciones oficiales de la "simulación" del agente encubierto que las justifique ya que están dadas en el marco de la previa autorización judicial dando cuenta inmediata al Juez de todo hecho relevante en la investigación. En el caso de que deba intercambiar material pornográfico infantil, este autor también considera como apropiado contar con la correspondiente autorización judicial especial para el caso.

Para finalizar, Vaninnetti también expresa su interés en legislar sobre la cuestión del llamado "ciberpatrullaje" hecho por un agente encubierto con el fin aleatorio de participar en foros o comunidades/círculos cerrados para las búsquedas o rastreos efectuados a ciegas hechas con identidad simulada para detectar delitos de este tipo penal (pornografía infantil en la red). Sostiene que esta cuestión es sin dudas debatible y que demandará claras disputas doctrinarias pero que son necesarias encarar puesto que ante la delincuencia informática se hace necesario plantearlas y crear nuevas formas de concepción en la investigación de las mismas, sin apartarse del marco referencial prioritario de los derechos y garantías constitucionales. Con respeto al tema del ciberpatrullaje, este autor concluye afirmando que "*la restricción clásica de que deben existir previos indicios serios judicialmente ponderados y autorizados para permitir operaciones de infiltración no siempre ha de ocurrir tajantemente en Internet, puesto que la volatilidad de la información y lo variable de la misma hacen que la tarea del agente encubierto designado debería poder efectuarse igualmente mediante monitoreos en la red (las llamadas prospecciones), de lo contrario se perdería un precioso tiempo para detectar tales prácticas ilícitas*".

Nuevas herramientas para la investigación del delito

Como ya hemos adelantado en diversos puntos del trabajo, a criterio de estos autores, para la investigación de determinados delitos complejos donde el ciberdelincuente toma recaudos para evitar su identificación, consideramos como necesaria la regulación de la figura del agente encubierto digital en Argentina

En relación al ámbito de aplicación y desde nuestro punto de vista, la figura no debe ser amplia -aplicable para la investigación de cualquier tipo de delito- sino más bien restringida, limitada a determinados delitos que por su importancia, por lo disvalioso de la conducta, ameritan la utilización de esta herramienta. En virtud de ello, opinamos que en principio debe ser limitado a aquellos delitos donde el bien jurídico afectado sea la integridad (sexual, psicológica o física) de un menor. Es decir, aplicable para casos de *grooming*, corrupción de menores, casos de trata, secuestros, entre otros, siempre que exista algún tipo de riesgo para un menor. Quizás a futuro, una vez probada la eficacia y los resultados positivos de la utilización del agente encubierto digital, pueda proponerse la utilización para otros delitos complejos de similares características en relación a su dificultad al momento de la investigación.

Adherimos a la postura en que el agente encubierto digital solamente debería ser utilizado previa autorización por parte de juez competente, o en determinados casos (por ejemplo urgencia), podría ser autorizado u ordenado por el fiscal que lleva adelante la a investigación, con posterior notificación al juez de la causa, para que siempre exista control judicial sobre las tareas realizadas.

En relación a los sujetos autorizados para llevar adelante dichas tareas consideramos apropiado que sólo puedan ser realizados por el personal de las fuerzas de seguridad, excluyendo la posibilidad que civiles puedan realizar este tipo de tareas, atento a las siguientes razones:

- Las fuerzas de seguridad tienen mejores posibilidades de ser controlados por sus superiores en relación a las acciones realizadas.
- Las fuerzas de seguridad están en mejores condiciones de comprender y manejar los "códigos" utilizados por los delincuentes, favoreciendo la actuación del agente encubierto digital.
- Las fuerzas de seguridad se encuentran en mejores condiciones de preparación psicológica para hacer frente a distintos tipos de situaciones (por ejemplo, cuando sea necesario intercambiar material de pornografía infantil).

Sobre este último punto, ante el caso que el agente encubierto digital necesite realizar intercambio de material ilícito a fin de obtener la confianza necesaria que le permita entrar en el círculo de intimidad del delincuente, consideramos que para llevar a cabo dichas acciones será necesario solicitar autorización especial por parte del juez de la causa, teniendo además especial cuidado en el material utilizado, con pautas de razonabilidad como por ejemplo tratar de utilizar material donde los afectados sean mayor edad, imágenes que no sean especialmente degradantes, y se trate de material ya difundido, procedente de intervenciones anteriores, entre otros.

Desde el aspecto práctico, opinamos que la figura no debe ser utilizada como una de las primeras medidas por parte del investigador, sino que debe ser una herramienta sólo para el caso que a través de la aplicación de otras diligencias clásicas de las investigaciones no se hayan obtenido los resultados esperados o suficientes como para avanzar en la causa.

Siguien con aspectos de la práctica del agente encubierto digital, debemos mencionar la posible necesidad de tener perfiles falsos previamente construidos, listos para ser utilizados en el marco de una causa judicial. El fundamento de la necesidad, será dotar de mayor nivel de credibilidad al perfil falso utilizado por el agente encubierto digital, que al momento de establecer contacto virtual con el delincuente, será observado por este último, analizando su credibilidad. A diferencia de lo que sucede con un agente encubierto tradicional, donde es

necesaria una historia inventada y el nivel de credibilidad depende de las habilidades sociales (entre ellas, mentir bien) del agente, en el mundo informático es posible "revisar" esa historia inventada. Por ello, consideramos que a fin de ganar en credibilidad y posterior confianza (aspecto esencial para que tenga éxito la tarea del agente encubierto) será necesario tener preconstituidas distintas identidades digitales, donde cada perfil debe tener una vida, una historia, una interacción con el medio donde se encuentra (redes sociales, foros, etc).

Con respecto a un posible obstáculo de esta herramienta, sería el caso que teniendo construidos los perfiles falsos con destino a las investigaciones, las plataformas de redes sociales decidan suspenderlo o bloquearlo por incumplimiento de las obligaciones legales (términos y condiciones), particularmente la obligacion de brindar información verdadera (nombre, imagen, etc.). Otro aspecto problemático, sería en relación a las imágenes utilizadas (ya que los nombres podrían ser inventados) en los perfiles, en donde recomendamos tener en cuenta la utilización de imágenes o videos con el menor impacto (en lo posible, sin ninguna consecuencia) para los derechos de terceros.

Por último y en relación a las ventajas sobre la utilización de un agente encubierto digital, diremos que a diferencia de la figura clásica, en el caso digital no se estaría poniendo en riesgo la integridad física del agente de seguridad, toda vez que todas las acciones siempre se realizarían a través de medios electrónicos, y con los recaudos de seguridad de la información que se consideren adecuados para el caso. Además, también a diferencia del agente encubierto clásico, la versión digital digital de la figura permitiría guardar un registro electrónico sobre todas las acciones realizadas (chats por ejemplo), que ante casos de dudas o eventuales cuestionamientos legales, posibilitará la realización de una pericia informática que revele lo efectivamente realizado por el agente de las fuerzas de seguridad.

Conclusiones

Para combatir delitos cada vez más complejos, y sobre todo cuando intervienen las nuevas tecnologías como medio para la comisión de los mismos, el Estado necesita adaptarse, actualizarse. En general, así concluyen los distintos trabajos y eventos relacionados con la delincuencia informática y cibercrimen, donde se muestran nuevas técnicas y modalidades utilizadas por los delincuentes que utilizan las nuevas tecnologías para su propio beneficio.

No es novedad afirmar que el contínuo avance de las nuevas tecnologías trae consigo nuevos desafíos. En el ámbito de la delincuencia, el crecimiento en la utilización de Internet brinda toda una nueva gama de formas y medios sobre los cuáles cometer delitos, aprovechándose de usuarios que diariamente acceden a Internet desde todo tipo de dispositivos (smartphones, tablets, notebooks, etc.). Este escenario trae como consecuencia un aumento de la población pasiva que potencialmente puede ser víctima de distintos tipos de ataques, aumentando las posibilidades para los delincuentes que utilizan la tecnología para llevar a cabo sus acciones.

Como se ha visto a lo largo del trabajo, la complejidad de determinados delitos, sobre todo aquellos en donde los delincuentes toman determinados recaudos para evitar ser identificados, hacen necesaria la adecuación o adaptación de las herramientas de investigación.

Por todo esto, coincidimos y ponemos de manifiesto la necesidad de contar con nuevas herramientas procesales que permitan a las fuerzas de seguridad, llevar a cabo investigaciones con un mayor nivel de eficacia, particularmente, de la regulación legal de la figura del agente encubierto digital o informático, destinado a la persecución de delitos graves, particularmente aquellos donde el bien jurídico afectado sea la integridad de un menor.

Bibliografía

[1] PANDA SECURITY, “El mercado negro del Cibercrimen”, 2010. Url: https://www.incibe.es/file/WcGUL21k467M0ex5BxJguQ, Consultado: 01/06/2016

[2] MINISTERIO DE SEGURIDAD DE LA NACIÓN ARGENTINA, “Operación Oliver: Desarticulan red internacional de pedófilos”, Url: www.minseg.gob.ar/operación-oliver-desarticulan-red-internacional-de-pedófilos, Consultado: 01/06/2016

[3] TOR Project; Tor Overview, Url: https://www.torproject.org/about/overview.html.en, Consultado: 01/06/2016

[4] Organización de Estados Americanos, Relatoría Especial para la Libertad de Expresión; Url: http://www.oas.org/ES/CIDH/EXPRESION/showarticle.asp?artID=25&lID=2, Consultado: 01/06/2016

[5] GOMEZ, Leopoldo Sebastián, "El delito de pornografía infantil"; 1ra. Edición, Buenos Aires, 2012. p. 100 a 104.

[6] RODRÍGUEZ CARO, María Victoria. “La infiltración policial: en el límite del Estado de Derecho. El inminente agente encubierto informático”. Noticias Jurídicas. Url: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10222-la-infiltracion-policial:-en-el-limite-del-estado-de-derecho-el-inminente-agente-encubierto-informatico, Consultado: 01/06/2016

[7] HISTORIA DE LA LEY 19.366 (D. OFICIAL 23 de Septiembre 1994) ESTUPEFACIENTES. Santiago, Chile, 1994, Vol. I, p.39

[8] RIQUELME PORTILLA, Eduardo. “El agente encubierto en la ley de drogas. La lucha contra la droga en la sociedad del riesgo”, en Revista Electrónica Política Criminal nº2, A2, 2006, p. http://www.politicacriminal.cl/

[9] SOLOGUREN INSUA, Felipe. “El agente encubierto: ¿Peligro o beneficio en Estados democráticos?. Universidad de Chile. Departamento de Ciencias Penales. 2008. Url: http://repositorio.uchile.cl/tesis/uchile/2008/de-sologuren_f/pdfAmont/de-sologuren_f.pdf, Consultado: 01/06/2016

[10] Boletín del Ministerio de Justicia - Gobierno Español. Año LXX. BMJ núm. 2186. Febrero 2186 - ISSN: 1989-4767 – www.mjusticia.es/bmj, Consultado: 01/06/2016

[11] VANINETTI, Hugo “Agente encubierto y la pornografía infantil en internet”, publicado en LA LEY, DJ 02/11/2011, Cita Online: AR/DOC/2722/2011, Consultado: 01/06/2016