UNIVERSIDAD SIGLO 21
La educación evoluciona

UNIVERSIDAD EMPRESARIAL SIGLO 21

AGENTE ENCUBIERTO DIGITAL Y LA INTELIGENCIA ARTIFICIAL

Carrera: Especialización en Cibercrimen

Alumno: Bergamin, Federico Javier

DNI N° 25.956.767

Mayo de 2024

Resumen

Nos encontramos atravesando una Revolución a raíz del gran avance de la informática y de las comunicaciones acaecido en las últimas décadas, de dimensiones comparables, sino mayores, con la Revolución Industrial que vio inicio en Inglaterra allá por el año 1780.

A solo un clic de distancia nos podemos comunicar, interactuar, contratar y relacionar con personas en toda la faz del planeta.

Ello trae aparejado innumerables ventajas, pero también ha dado pie al avance de aquéllas organizaciones e individuos que, al amparo del anonimato que puede verse favorecido por este tipo de interacción, se dedican a la realización de ilícitos.

Muchos de ellos son de naturaleza económica, habiendo sido un terreno propicio para el afincamiento de estafadores que, mediante el uso de la ingeniería social, engañan y desapoderan a sus víctimas que, muchas veces, ni siquiera acuden a formular la denuncia ante las autoridades, por diversos motivos.

Ahora bien, también los agresores sexuales han visto en Internet un campo propicio para contactar futuras víctimas, sobre todo menores de edad.

Es así que las autoridades tienen la obligación de *aggiornarse* a estas nuevas modalidades delictivas, por lo que en el presente trabajo propugnaremos la utilización de una figura antigua, como lo es la del agente encubierto, pero adaptada a las nuevas necesidades, es decir, para actuar en la web, en las redes sociales y en las salas de chat.

Por lo demás, y teniendo en cuenta los avances de la I.A. (Inteligencia Artificial) y el uso de bots, es que también se propondrá la utilización de estas herramientas y medios para suplantar a las personas físicas que históricamente se han encargado de estas tareas, lo que

redunda en grandes beneficios, no sólo económicos sino también en cuanto a la eficacia, para los Estados involucrados.

Además, las mencionadas herramientas son de gran utilidad para un eventual ciberpatrullaje coordinado de todos los Estados firmantes del Convenio de Budapest, a fin de lograr el desbaratamiento de organizaciones criminales que, al amparo del anonimato de Internet y de la Deep Web, intercambian material de abuso sexual infantil. Para ello, se propone la creación de una biblioteca de dichas imágenes con su respectivo código HASH, a fin de que, de manera automatizada, dichos bots y/o Inteligencia Artificial al servicio de los Estados, busque de manera permanente a usuarios que almacenen, transfieran o comercialicen dicho material.

Las bondades de la nueva era traen aparejados nuevos desafíos. Es deber de los Estados estar a la altura.

Palabras Clave

Agente Encubierto, Ciberpatrullaje, Evidencia Digital, Canales abiertos, Canales Cerrados, Evidencia digital.

.

Abstract

We are going through a Revolution as a result of the great advance in computing and communications that has occurred in recent decades, of comparable dimensions, if not greater, with the Industrial Revolution that began in England back in 1780.

Just a click away we can communicate, interact, hire and relate to people all over the face of the planet.

This brings with it innumerable advantages, but it has also given rise to the advancement of those organizations and individuals who, under the protection of the anonymity that can be favored by this type of interaction, are dedicated to carrying out crimes.

Many of them are economic in nature, having been a favorable terrain for the establishment of scammers who, through the use of social engineering, deceive and disempower their victims who, many times, do not even come to file a complaint with the authorities, for various reasons.

Now, sexual offenders have also seen the Internet as a favorable field for contacting future victims, especially minors.

Thus, the authorities have the obligation to embrace these new criminal modalities, which is why in this work we will advocate the use of an old figure, such as that of the undercover agent, but adapted to the new needs, that is, to act on the web, on social networks and in chat rooms.

For the rest, and taking into account the advances of A.I. (Artificial Intelligence) and the use of bots, is that the use of these tools and means will also be proposed to supplant the natural persons who have historically been in charge of these tasks, which results in great benefits, not only economic but also in regarding effectiveness, for the States involved.

Furthermore, the aforementioned tools are very useful for an eventual coordinated cyber patrol of all the signatory States of the Budapest Convention, in order to achieve the disruption of criminal organizations that, under the protection of the anonymity of the Internet and the Deep Web, exchange material of child sexual abuse. To this end, the creation of a library of said images with their respective HASH code is proposed, so that, in an automated manner, said bots and/or Artificial Intelligence at the service of the States, permanently search for users who store, transfer or commercialize said material.

The benefits of the new era bring new challenges. It is the duty of the States to live up to it.

Keywords

Undercover Agent, Cyber Patrolling, Digital Evidence, Open Channels, Closed Channels, Digital Evidence.

INDICE

1 INTRODUCCIÓN

Los agentes encubiertos han constituido la primera línea ofensiva en la lucha contra la criminalidad organizada.

Es sabido que las distintas asociaciones criminales tienen una naturaleza intimista, es decir, se forman y se basan en torno a relaciones familiares, de amistad o de pertenencia a un grupo social caracterizado por su cultura, lengua, religión o étnica, sumado al carácter encubierto de sus actividades, en donde rige un código de secreto estricto.

Por ende, es necesario el diseño de una política criminal que tienda a la prevención, investigación y sanción de estas organizaciones criminales que se adecúe a esa realidad criminal, surgiendo así la figura del agente encubierto como idónea para introducirse en las mismas de manera oculta, es decir, infiltrarse, para así desde el interior de la misma, descubrir su modus operandi, funcionamiento, miembros, destino del dinero y demás objetos e instrumentos del delito, con el fin último de desbaratarla.

1.1. El derecho y su necesaria adaptación a la nueva realidad social y tecnológica

Nadie puede poner en duda la rápida evolución de las tecnológicas de la información y de la comunicación (T.I.C.), sumado al surgimiento de nuevos entornos virtuales de interacción social, y la proliferación en el uso de instrumentos tecnológicos (Salt & Polansky, 2023).

Decía Paul Freund, ilustre jurista norteamericano del siglo XX y que fue varias veces candidato a la US Suprem Court, que el Tribunal Supremo "no debía dejarse influenciar por el tiempo del día, pero inevitablemente sería influenciado por el clima de la era" (Salt & Polansky, 2023).

La necesidad de la progresiva adaptación del derecho se plasma en la Sentencia del Tribunal Superior español N° 173/2018 de 11 de abril. Aquí se valoró que se encuentran en pugna ciertos derechos del investigado, tales como el derecho al entorno virtual, el derecho a la intimidad, el derecho a la autodeterminación informativa, el derecho a la inviolabilidad del domicilio en caso de agentes encubiertos convencionales, y el derecho a no declarar contra sí mismo y no confesarse culpable. Sin embargo, dicha resolución descartó la afectación del derecho al secreto de comunicaciones (art. 18.3, CE) toda vez que "uno de los comunicantes es el propio agente. No hay inmisión en una comunicación que establecen terceros, sino comunicación entre agentes y recurrente que no precisa habilitación judicial ex art. 18.3, CE".

> El mundo ha cambiado, las formas de comunicarse se han multiplicado, y todo este complejo paradigma se ha traducido también en el desarrollo de una nueva dimensión sociológica sobre la que han de ser interpretados los derechos fundamentales, Por ello, casos como los planteados en la STS 173/2018 han de ser abordados desde la perspectiva del nuevo mundo tecnológico. Solo de esta manera es posible entender que la intromisión de un agente infiltrado en un ámbito de comunicación en el que cientos de personas intercambian ideas u opiniones constituye una monitorización de decenas de procesos comunicativos que implica una interferencia en el derecho al secreto de comunicaciones de todos aquellos (Salt & Polansky, 2023, pág. 220).

Lo cierto es que, en la persecución y averiguación de la criminalidad, ésta siempre va un paso adelante en la utilización de cuantas herramientas están a su alcance. Ello se debe, en gran parte, a carecer de impedimentos económicos, ni legales, ni éticos ni de cualquier otra índole.

En contrapunto, estamos en condiciones de afirmar que la Justicia siempre va un paso detrás en la incorporación de medios técnicos, digitales y de cualquier otra índole (Fuentes, 2024).

La lucha contra la criminalidad el terrorismo y ciberdelincuencia, así como la ineludible necesidad de desarrollar las herramientas necesarias para combatirlos ha dado lugar al reconocimiento de la necesidad de medidas tecnológicas de investigación encubierta (Fuentes, 2024).

La globalización, sobre todo en relación a la economía, ha dado paso a la expansión de estos grupos de criminalidad, logrando traspasar las fronteras nacionales, haciendo ineficaces muchos de los instrumentos de investigación utilizados tradicionalmente por el Estado de Derecho para combatir este tipo de delincuencia (Fuentes, 2024).

Además, debemos tener en cuenta la aparición de nuevos espacios de actuación que so utilizados por los ciberdelincuentes para sortear las barreras ordinarias de control, tales como la existencia de la Deep Web, o el uso de criptomonedas que torna de casi imposible seguimiento y/o rastreo a las transacciones comerciales, o la utilización de técnicas de enmascaramiento de las desde las cuales se accede a la internet, que evita la posibilidad de establecer la terminal de conexión y, por ende, la identidad y localización de los autores.

Es de fundamental importancia hacer mención en este punto al **Convenio sobre Ciberdelincuencia del Consejo de Europa**, suscrito el 23 de noviembre de 2001 en la ciudad de **Budapest** –más conocido como *Convenio de Budapest*– que busca establecer una legislación penal y procedimientos comunes entre los países suscriptores, para perseguir delitos cometidos a través de medios electrónicos e informáticos.

También busca fomentar y fortalecer la cooperación internacional en esta materia; destaca la necesidad de aplicar una política penal común para perseguir esta clase de delitos;

busca armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país; como así también establecer un régimen rápido y eficaz de cooperación internacional.

1.2. Antecedentes históricos de la figura del agente encubierto

La figura del agente en cubierto no es novedosa, sino que, al contrario, ha sido utilizada desde hace siglos para las investigaciones de delitos complejos.

El origen del agente encubierto es discutido. Para algunos autores, alusiones a esta figura se contendrían en los relatos bíblicos, particularmente en el Génesis (III, 1-7). Para otros, el origen de esta figura estaría en la antigüedad griega, en las fábulas de Esopo (Esopo, III, fábula V, Aesopus et petulans) (Insua, 2024).

Coincide la doctrina en señalar que el origen del agente encubierto está en la expresión francesa “Agent provocateur”, y que se utilizó para referir a actividades de espionaje político surgidas en Francia bajo los Gobiernos de Luis XIV y Luis XVI, en la que determinados “agentes” agentes” promovían disturbios, atentados, con el objetivo de crear un estado en la que se fundamentaran medidas de persecución contra los enemigos del régimen absolutista. En esta época, los agentes de policía francesa inducían a otros a cometer delitos políticos con el objetivo de eliminar a individuos que eran vistos como peligrosos por el Gobierno (Insua, 2024).

La institución pasó del espionaje a la provocación.

Los espiones de la policía se denominaban mouches o mouchards, se dividían en: i) aquellos que trabajaban clandestinamente para los inspectores (observateur) y ii) aquellos que operaban abiertamente, sujetos que habían estado detenidos, y que obtenían su libertad a cambio de colaboración (mouches). Las fuerzas del orden revolucionario, utilizaron agentes

provocadores para descubrir los complots en las prisiones, los cuales se denominaban moutons de prisons (Insua, 2024).

Uno de los casos más famosos de actividad encubierta fue el protagonizado por el agente federal Joe Pistone en los Estados Unidos quien, bajo el seudónimo de Donnie Brasco, logró infiltrarse en la mafia ítalo-americana durante seis años y de esta manera logró obtener información vital para ser utilizada en contra de los integrantes de la Cosa Nostra de Nueva York (Aboso, 2023).

Los elementos probatorios que recaudó Pistone fueron de tal magnitud que alcanzaron a la Fiscalía de aquel entonces para llevar a juicio a los integrantes de dicha organización, y obtener severas condenas, con lo cual se logró desbaratar la misma.

1.3. Cuestionamientos a la figura del Agente Encubierto

No escapa a los autores que tratan la figura del agente encubierto que ésta ha sido seriamente cuestionada, sobre todo desde el punto de vista ético y de su constitucionalidad. Lo que no se discute es que estamos ante una herramienta exitosa para la investigación, que le ha traído numerosos provechos al Estado.

La legislación internacional y nacional, en los últimos tiempos y bajo el rótulo de un presunto estado bélico denominado “guerra contra la delincuencia”, ha tendido a autorizar, para la investigación de ciertos delitos generalmente considerados complejos (narcotráfico, tráfico de armas, trata de personas, etc.) o graves (secuestro extorsivo), la utilización de determinada figuras denominadas medios extraordinarios de prueba que, por su poder lesivo para los derechos subjetivos, han despertado serios interrogantes acerca de su constitucionalidad y/o convencionalidad.

La actuación encubierta consiste en la actividad cumplida por una persona cualquiera o por un funcionario de la policía que, simulando ser un delincuente, se introduce en una organización delictiva con el propósito de proporcionar, desde el interior de la misma, información acerca de ella que permita evitar el delito o su descubrimiento, la individualización de sus integrantes, en su caso su detención, el desbaratamiento de la misma, la obtención y/o custodia de pruebas y el enjuiciamiento de sus miembros (Pascua, 2018).

Al respecto podemos encontrar dos grandes grupos de autores, unos que justifican la legalidad de estos institutos, y otros que los tachan de inconstitucionales y/o inconvencionales.

Entre quienes lo aceptan, indican que el instituto del agente encubierto, en la lucha contra el crimen organizado y ante los delitos complejos por él producidos, el Estado se encuentra en desventaja o imposibilitado de hacerle frente, quedando la sociedad en estado de indefensión si sólo se conduce con las vías probatorias ordinarias.

Por otro lado, quienes critican su regulación legal señalan que se busca con este instituto legitimar la ilegalidad en la investigación penal estatal, como medio no tan novedoso, como ilegalmente explícito, para dar más eficacia respecto de aquellos delitos. En este orden de ideas, Marcelo Sancinetti postula que la primera cuestión es si estos institutos violan o no derechos del imputado. Si no los violan, los puede hacer valer el Estado sin tener que echarle la culpa a la víctima. Y si los viola, no se les puede hacer valer en el proceso, aunque se invoquen derechos de la víctima (Pascua, 2018).

En definitiva, quienes abogan por la inconstitucionalidad de estas figuras señalan que con su pretendida implementación se trastoca el derecho de defensa en juicio en general, y en particular el debido proceso legal, ya que señalan que el Estado no puede combatir el delito cometiendo delitos.

1.4. Modos de ingresar a la criminalidad organizada

En este punto analizaremos cómo los miembros de una organización criminal reclutan nuevos integrantes, y en particular, de qué modo buscan asegurarse que no pertenezcan a fuerzas oficiales de investigación, es decir, personal policial que actúa como agente encubierto.

> Las contramedidas adoptadas por las asociaciones criminales suelen consistir en hacer partícipes de sus actividades delictivas a todos sus miembros y – en especial – a los nuevos, en donde muchas veces incluye el asesinato como una forma de comprobar la fidelidad del aspirante al grupo criminal. Entre las medidas para evitar esas infiltraciones que implementan las organizaciones criminales se cuenta también el reclutamiento de integrantes de una misma familia, de un mismo extracto social, incluso de una misma etnia de pertenencia. Las modernas organizaciones criminales dedicadas al tráfico ilegal de estupefacientes, trata de personas, tráfico de armas, incluso el terrorismo, operan desde hace tiempo con estos estándares que minimizan los riesgos de una infiltración exitosa por parte de las autoridades públicas (Aboso, 2023, pág. 391).

Como se puede advertir, las organizaciones criminales buscan hacer delinquir a quien pretenda ingresar y convertirse en miembro de las mismas, como prueba de fidelidad y de que no están ante un agente del Estado.

La Convención de las Naciones Unidas contra la Delincuencia Organizada del año 2000 establece, en su art. 20, las técnicas especiales de investigación para los delitos cometidos en el ámbito de la criminalidad organizada. El párrafo primero de ese artículo 20 dispone:

"1. Siempre que lo permitan los principios fundamentales de su ordenamiento jurídico interno, cada Estado Parte adoptará, dentro de sus posibilidades y en las condiciones prescritas por su derecho interno, las medidas que sean necesarias para permitir el adecuado recurso a la entrega vigilada y, cuando lo considere apropiado, la utilización de otras técnicas especiales de

investigación, como la vigilancia electrónica o de otra índole y las operaciones encubiertas, por sus autoridades competentes en su territorio con objeto de combatir eficazmente la delincuencia organizada".

En el caso de la República Argentina, la ley 27.319 ha venido a regular distintas técnicas de investigación aplicables a delitos complejos. Esa ley debe ser relacionada, desde el punto de vista de las metas de eficacia del resultado de la investigación, con la sanción de la ley 27.304 que modifica el sentido y el alcance de la figura del arrepentido en la legislación penal nacional (Aboso, 2023).

2 EL AGENTE ENCUBIERTO

Los estados cuentan con diversas herramientas para combatir el crimen organizado. Entre ellas, podemos destacar las intervenciones telefónicas, los allanamientos remotos, el bloqueo de activos ilegales, el rastreo de fondos ilícitos, pero una de las fundamentales es la actuación de los agentes encubiertos.

En efecto, si hablamos de uno de los mayores flagelos a nivel mundial, y uno de las actividades ilícitas que mayores masas de dinero ilegal mueve en el mundo como es el tráfico ilegal de estupefacientes, podemos aseverar que la utilización de la figura en cuestión – el agente encubierto – ha resultado una herramienta de alta utilidad para investigar esta forma de criminalidad organizada.

¿De qué hablamos cuando nos referimos a “agente encubierto”? Al decir de Aboso (2023) “el concepto de agente encubierto está inexorablemente vinculado con la actuación de un funcionario público que simula ser un integrante de una organización criminal con el objeto de descubrir sus actividades ilícitas, identificar a los responsables y aportar prueba de cargo al proceso penal para imponer sanciones”.

En todas las legislaciones del orbe se ha previsto que el agente encubierto sea un funcionario público altamente calificado. Ello se debe a que se exige de estos “un grado de profesionalismo y dedicación superior que excede con creces el cumplimiento de los deberes ordinarios, puesto que se requiere una dedicación total y el dominio del arte de la simulación” (Aboso, 2023, pág. 366).

La figura del agente encubierto se encuentra regulada prácticamente en todas las legislaciones modernas del mundo, como ser Alemania, España, Holanda, Inglaterra, etc.

En Argentina se introdujo la figura mediante Ley 24.424 (1995) que modificó la Ley de Estupefacientes N° 23.737, introduciendo en los arts 31 bis a 31 quinquies la figura del agente encubierto.

Allí se faculta al juez a recurrir al uso de agente encubierto con el propósito de "comprobar la comisión de algún delito previsto en esta ley o en el art. 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".

Posteriormente, esa normativa fue modificada por la ley 27.319, denominada "Delitos complejos", que amplió el horizonte normativo, antes limitado a la lucha contra el tráfico ilegal de drogas, por un nuevo escenario que incluyó también delitos aduaneros, delitos de terrorismo, delitos sexuales, delitos contra la libertad, delitos contra el patrimonio, delitos de trata de personas, delitos de asociación ilícita y los delitos que atentan contra el orden socioeconómico. En particular, el art. 30 de esa ley regula la figura del agente encubierto.

Art. 3. Será considerado agente encubierto todo aquel funcionario de las fuerzas de seguridad autorizado, altamente calificado, que presta su consentimiento y ocultando su identidad, se infiltra o introduce en las organizaciones criminales o asociaciones delictivas, con el fin de identificar o detener a los autores, partícipes o encubridores, de impedir la

consumación de un delito, o para reunir información y elementos de prueba necesarios para la investigación, con autorización judicial.

Como venimos afirmando, está claro que la finalidad de esta figura es la de “obtener medios de prueba que permitan identificar o detener a los partícipes de esa clase de asociaciones criminales, o de impedir la consumación de un delito” (Aboso, 2023, pág. 371).

A diferencia de la anterior regulación, la decisión de introducir un agente encubierto en una asociación delictiva depende del juez, pero con intervención del fiscal (Aboso, 2023).

2.1 Agente encubierto y Agente provocador

Es menester formular la distinción entre estas dos figuras, puesto que la doctrina en ocasiones las ha confundido.

Esta tarea es necesaria en razón de que, si bien se ha discutido la constitucionalidad y/o convencionalidad de la figura del Agente Encubierto sin mayor éxito, no ha sido el mismo resultado con la figura del Agente Provocador, siendo ésta última mucho mas cuestionada y, por ende, de dudosa constitucionalidad.

> En la actuación de un agente encubierto es patrimonio común la distinción de una infiltración de larga duración de otra de corto período de tiempo. Respecto de esta última, la doctrina y la jurisprudencia se refieren a ella con la denominación de "agente provocador", en donde el funcionario policial, ocultando su calidad, participa en una actividad delictiva (Aboso, 2023, pág. 367).

Estamos ante un *agente provocador* en aquellos casos en que el funcionario estatal simula un interés en la adquisición de un producto de origen ilícito, tales como armas, drogas, explosivos o precursores químicos, con el objetivo de acercarse a aquéllos integrantes de la

organización delictiva que se dedican a la venta y, así, desenmascararlos, aprehenderlos e intentar ir por las autoridades superiores de la organización, que suele tener estructura piramidal.

Distinta es la figura del “agente encubierto”, en donde el agente estatal, generalmente funcionario policial especialmente capacitado, cuenta con autorización judicial para enmascarar su identidad y función frente al público en general y por un lapso de tiempo determinado, tendiente a infiltrarse en una organización criminal, detectar su existencia o no como tal, su funcionamiento, sus miembros, su vía de canalización de ingresos y activos, con la finalidad ulterior de informar a las autoridades para el desbaratamiento de la misma.

Además, el agente encubierto va a tener la posibilidad de ir recabando distintos elementos de prueba, que van a servir al Agente Fiscal para llevar a juicio a los integrantes de la organización, para lo cual debe cuidarse en todo momento de no vulnerar garantías constitucionales ya que, de lo contrario, va a ser procedente el instituto de la exclusión probatoria en el marco de un proceso, y no podrán ser utilizadas las probanzas obtenidas con tanto esfuerzo.

> “La calidad de funcionario público del agente encubierto lo distingue de otro mecanismo de investigación para delitos complejos como lo es el agente informante. Este no guarda ninguna relación formal o funcional con los organismos de seguridad y de investigación, siendo su cometido principal el de aportar información útil para descubrir las actividades de una organización criminal, identificar a sus responsables y/o aportar pruebas idóneas para llevar a juicio a sus integrantes. Su tarea está motivada generalmente por el lucro y su actividad suele constituir uno de los pilares sobre los que se asienta la moderna investigación penal de delitos complejos” (Aboso, 2023, pág. 394).

El fundamento de la regulación de esta figura radica, precisamente, en la dificultad con que cuentan los estados para desenmascarar a las organizaciones criminales. Es decir, éstas actúan – precisamente – de manera encubierta, con actividades lícitas como "pantalla".

Además, suelen estas organizaciones reclutar a sus miembros teniendo en cuenta personas que hablan la misma lengua, o que tienen vínculos familiares cercanos, e incluso que vivan en zonas aledañas, con lo cual, la infiltración a estas es sumamente dificultosas.

Si a ello le sumamos las distintas *pruebas* que obligan a realizar a los candidatos que pretenden ingresar a las mismas, nos encontramos con claridad ante las dificultades con que va a tener un agente policial para la investigación de estas.

No basta con que el agente encubierto adopte un nombre apócrifo para que el ingreso a la organización sea exitoso. Va a tener que también munirse de documentación falsa expedida por la autoridad competente, algún antecedente criminal, como así también personas que refieran conocerlo del ámbito del hampa, a fin que el acto de engaño tenga posibilidades de ser exitoso. En ocasiones se ha utilizado a *arrepentidos*, es decir, miembros de la organización que pactan con el Agente Fiscal a cambio de morigeración en su situación procesal, para que sean éstos quienes introduzcan a modo de presentación a los agentes encubiertos, a los líderes y/o reclutadores de la organización delictiva.

"Es decir, existe un trabajo previo sobre los perfiles personal, social y económico del funcionario público que actúan bajo esa tapadera que deben ser minuciosamente conformados para evitar una delación involuntaria" (Aboso, 2023, pág. 372).

2.2 La figura del Agente Encubierto en la lucha contra el M.A.S.I. (Material de abuso sexual infantil)

Cuando hay niños y niñas involucrados no es correcto hablar de pornografía.

Cuando hablamos de M.A.S.I. aludimos al “material sobre abuso sexual infantil que opera como materia prima de un modelo de negocio sostenido por abusadores sexuales que producen, difunden y comercializan contenidos íntimos de niñas o niños, vulnerando sus derechos” (Digital, 2024).

Ingresando al núcleo de este trabajo, trataremos ahora el tema del agente encubierto informático, que se ha convertido en una herramienta novedosa y fundamental para la lucha contra la distribución de M.A.S.I. (material de abuso sexual infantil).

Resulta sumamente difícil ganarse la confianza de un pedófilo en las redes sociales y/o grupos de chat donde suelen merodear e intercambiar material, a la vez de captar menores para lograr generar el contenido ilícito que luego distribuyen y/o comercian.

Es así que los pedófilos han adoptado diversos mecanismos de control y/o de validación de intereses comunes con aquéllos con quienes habrán de intercambiar material. No hablamos aquí de validación de identidad, puesto que el anonimato es la regla de oro de estos abusadores virtuales, ya que jamás develan sus nombres reales, actuando en la clandestinidad y en las condiciones de ocultamiento de identidad que favorece el uso de internet, enmascarando generalmente sus IP, adoptando Nick names que nada tienen que ver con su identidad real, como así también utilizando VPN que impiden determinar su ubicación geográfica.

Es realmente un desafío para las autoridades la investigación de estos delitos por las dificultades a las que estamos aludiendo, no obstante, lo cual la combinación de la figura que venimos estudiando, juntamente con el allanamiento remoto y el ciberpatrullaje digital realizado por Inteligencia Artificial, se erigen en novedosas y eficientes herramientas para la lucha contra estos flagelos.

Tal como vengo argumentando, para ser aceptado en un grupo donde se intercambia material de este tipo, los administradores suelen solicitar al aspirante a ingresar que éste envíe imágenes de abuso sexual infantil. Así, y solo así, podrá ser aceptado como miembro.

De este modo se aseguran, por un lado, que la persona que quiere ingresar tenga intereses afines a este grupo de ofensores sexuales. Por otro lado, con el conocimiento que tienen de que dicha actividad es claramente ilegal, para el ingreso al grupo común exigen la comisión de un ilícito, como modo de aseguramiento que no se está ante un agente policial.

La ley 27.319 es la que faculta al Agente Fiscal a solicitar al Juez de Garantías que se nombre un funcionario policial en carácter de agente encubierto, para así "pesquisar el tráfico ilegal de material pornográfico prohibido" (Aboso, 2023, pág. 372).

Si bien la figura del agente encubierto informático está especialmente pensada en la actualidad para combatir delitos tales como el intercambio y/o producción de material de abuso sexual infantil y el Grooming, también puede ser utilizada la figura para investigar delitos de otro tipo que tienen que ver también con organizaciones criminales, muchas veces transnacionales, como puede ser el comercio legal de estupefacientes, la venta de armas de fuego, posibles atentados terroristas, estafas u otras formas de actividades ilícitas que utilizan internet como medio para cometer tales ilícitos.

Son de utilidad para el análisis de la figura en cuestión las estadísticas que ha relevado el sitio web Faro Digital, obtenidas de información brindada por el Ministerio Público Fiscal de la provincia de Buenos Aires.

> En 2021 fueron 29,3 millones las denuncias relacionadas con material pedófilo y sospechas de explotación sexual infantil.
>
> El crecimiento anual del contenido pedófilo generado por niños y niñas creció anualmente un 374% (2021).

82% agresores son hombres; 9%, mujeres.

78% de víctimas que denuncian son niñas; 15%, niños.

80% de las denuncias en Argentina se dieron a partir de talleres de ESI en la escuela. Fuente: Ministerio Público Tutelar (Digital, 2024).

2.3 El agente encubierto digital en España

En España la figura del agente encubierto había resultado de suma utilizada históricamente en la investigación de delitos tales como tráfico de estupefacientes. No obstante, atento a los avances tecnológicos, era necesario *aggiornar* la legislación.

Es por ello que en el año 2015 se sancionó una ley que previó que es el Juez de instrucción quien se encuentra facultado a 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 algunos delitos específicos.

Además, se autorizó expresamente al agente encubierto informático a intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, y a analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.

Asimismo, y siempre en el marco y 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 (Salt & Polansky, 2023).

La intromisión de un agente encubierto en un canal cerrado de comunicación podría suponer no solamente una afección del principio de prohibición de interdicción en la arbitrariedad de los poderes públicos, sino también del derecho a la intimidad y al

> secreto de comunicaciones de los sujetos intervinientes en el citado canal cerrado de comunicación (Salt & Polansky, 2023, pág. 224).

Como vemos, en España se autoriza por vía de ley al agente encubierto a enviar archivos ilegales en el marco de su actuación, previendo la situación a la que ya hemos aludido, en que los administradores de estos canales cerrados tienden a verificar el grupo de pertenencia y lealtad de los nuevos miembros mediante la exigencia del envío de este material. Así, el agente encubierto puede realizar las medidas tendientes al ingreso sin violentar la ley.

El envío de estos archivos ilícitos plantea una de las cuestiones más complejas de la actividad del agente encubierto informático, cuando se trata de material de abuso sexual infantil.

La tenencia y el intercambio de estos archivos no plantea problema alguno, ya que el agente encubierto online está exento de responsabilidad criminal. La cuestión radica en que el investigado-delincuente le va a exigir la remisión de dicho material para permitirle ingresar a los foros cerrados, y no le va a ser posible al agente encubierto entregar material ya creado por otros criminales pedófilos, pues los nombrados manejan, tienen y hacen circular la mayoría de las reproducciones (imágenes, videos) ya existentes, con lo cual va a ser imprescindible que – para tener éxito en su gestión – aporten material nuevo.

Es que estas comunidades de pederastas son en extremo desconfiadas de los “nuevos miembros”, y exigen *algo* de ese material para verificar que tengan del otro lado a persona con los mismos gustos perversos que ellos.

Por supuesto que no se van a poder crear imágenes reales de niños siendo abusados para intercambiar. No obstante, sí se podría acudir – y efectivamente se ha hecho – a simulaciones de jóvenes, realizadas por adultos.

Para estos casos, hasta un límite de edad se ha utilizado la imagen de adultos con aspecto aniñado o infantil, tanto actores como miembros de la Policía.

No obstante, si se le exige al agente encubierto, el envío de material *nuevo* de niños de corta edad, la cuestión se complica.

Ahora bien, los avances tecnológicos, y sobre todo, la Inteligencia Artificial, han permitido la creación de imágenes infantiles para ser utilizadas como moneda de cambio con los pedófilos.

El intercambio de archivos ilícitos, siempre y cuando la intención delinquir haya partido previamente del sujeto investigado, no puede ser considerado como provocación del delito.

3 AUTORIZACIÓN JUDICIAL Y AMBITO DE ACTUACIÓN

Es insoslayable la autorización judicial para que un agente encubierto pueda actuar válidamente como tal.

Así, será el Agente Fiscal quien evalúe la pertinencia, utilidad y necesidad de la medida y, en caso de concluir de manera afirmativa, solicitará al Juez de Garantías que corresponda en forma fundada la autorización para que se disponga la utilización de la figura aludida.

> Las captaciones y registros realizados por el agente encubierto gracias a los adelantos de la tecnología de las conversaciones personales, telefónicas o de cualquier otra naturaleza que mantenga con el acusado con el objeto de ser utilizado en el proceso judicial como prueba incriminante también deben estar autorizadas judicialmente (Aboso, 2023, pág. 391).

Tal como vengo afirmando, la utilización de la figura del agente encubierto está exclusivamente prevista para ser utilizada en el marco de delitos complejos o de difícil

investigación. Así, la ley 27.319 establece un sistema de número cerrado (numerus clausus) a fin de determinar aquellos delitos que pueden ser investigados con el uso de esta modalidad.

Será el Agente Fiscal quien evalúe la razonabilidad y proporcionalidad para disponer se requiera autorización al Juez para la implementación de la figura en el caso en cuestión, puesto que no bastará que se esté ante un caso complejo o de difícil investigación para que automáticamente se eche mano de la figura del agente encubierto.

Tenemos que pensar en dificultades superlativas en materia probatoria que hagan necesario el uso de agentes encubiertos (Aboso, 2023).

> En ese sentido, será el juez, en su papel de garante del proceso, el que deberá analizar puntualmente las circunstancias que rodean al pedido fiscal y los escollos prácticos que se presentan para el desarrollo del proceso. También deberá analizar en el caso concreto los riesgos potenciales del uso de un agente encubierto y las posibilidades de su detección temprana, con el riesgo inherente para su integridad física (Aboso, 2023, pág. 395).

3.1 El principio de irresponsabilidad del Agente Encubeirto

El agente encubierto deberá, en el marco de su actuación, posiblemente acceder a la comisión de algún o algunos hechos ilícitos, vinculados con la investigación.

Avanzando con la temática que nos ocupa, diremos que aquél funcionario devenido en agente encubierto por autorización judicial que pretenda hacerse pasar en un simple navegador de internet y así ingresar en un grupo de pedófilos, ya sea de WhatsApp, de Facebook, de Instagram o de Telegram por citar los más usuales, a fin de lograr la ulterior identificación de todos aquéllos que pertenezcan a dicho grupo e intercambien imágenes de M.A.S.I. y así reunir

prueba de cargo, le será exigido – a fin de lograr el acceso a ese grupo – que envíe material de M.A.S.I.. De este modo, los administradores del grupo buscan fidelizar los ingresantes y evitar las intromisiones de la autoridad.

Idéntica situación se da en el mundo no virtual, es decir, en el mundo real. Aquellos reclutadores de miembros de la organización delictiva le van a exigir al pretenso ingresante la comisión de un ilícito, a fin de así probar su lealtad y voluntad de ingreso. Así, se le suele exigir que trasporte estupefacientes de un lugar a otro a modo de prueba de fuego para ingresar a una organización criminal dedicada a ello, e incluso se les ha llegado a exigir que se le de muerte a una persona para acceder a organizaciones más violentas, como aquéllas que se dedican al sicariato o al terrorismo.

He aquí uno de los principales problemas de la figura del agente encubierto.

> Mientras que la comisión de ciertos delitos podrían estar alcanzados por el cumplimiento del deber, por ejemplo, su participación en el tráfico ilegal de drogas o el envío de material pornográfico infantil, en otras hipótesis el ejercicio de ese deber tiene límites a veces imprecisos, por lo que corresponde analizar si la participación del funcionario público que actúa a modo encubierto en un robo, secuestro, o directamente en un plan homicida puede estar justificado o no a la luz del derecho vigente (Aboso, 2023, pág. 398).

Así, se ha dicho que “en principio, debemos señalar que la ley no debe autorizar la afectación de bienes jurídicos para lograr la protección de bienes jurídicos, lo que ya por sí solo aparece como una flagrante contradicción in terminis” (Aboso, 2023, pág. 398).

Cuando los delitos que el agente encubierto comete son de escasa entidad, el Agente Fiscal suele aplicar criterios de oportunidad, evitando así el ejercicio de la acción penal a su respecto. Ello, en razón que la actuación del mismo estuvo encaminada a la investigación de

delitos de mayor gravedad cometidos por miembros de la organización delictiva a la que se pretende desbaratar.

Puede suceder que el agente encubierto se encuentre en una disyuntiva de conflicto de deberes, puesto que por un lado debería actuar para impedir la comisión de ilícitos, en tanto que por el otro lado tiene la obligación funcional de actuar para investigar a la organización. Estos son problemas que encuentran solución en la evolución actual de la Teoría del Delito, más precisamente en el ámbito de la antijuridicidad o de la culpabilidad, puesto que sin dudas nos encontramos ante conductas típicas, no obstante lo cual no será punible el funcionario policial actuando de encubierto.

Es la propia ley 27.319 que prevé la exención de responsabilidad criminal por los delitos cometidos en el marco de la investigación encubierta, siempre y cuando no se hubiese generado un peligro concreto para la vida, integridad física o psíquica de una persona.

3.2 Limitaciones a la Actuación del Agente Encubierto

Debemos tener en claro que el agente encubierto no puede inducir a otros a la comisión de un delito. Su función principal y excluyente radica en obtener elementos de cargo para que el Agente Fiscal pueda eventualmente llevar a juicio a los integrantes de la organización, con el fin de desbaratarla.

En el camino del agente encubierto no pueden existir acciones ilegales que consistan en haber provocado que otros cometan delitos. Esto es lo que lo diferencia del agente provocador, que ha sido cuestionado en su constitucionalidad por la gran mayoría de la doctrina.

El Estado no puede valerse de provocar a otros para que cometan delitos a fin de ulteriormente ser investigados. Nunca el Estado podría promover la comisión de hechos ilícitos.

Como tiene dicho el Tribunal Europeo de Derechos Humanos, el interés público no puede justificar el uso de evidencia obtenida como resultado de una provocación policial, de lo contrario, se expondría al acusado al riesgo de ser privado definitivamente de un juicio justo (Aboso, 2023) .

Para que sea válida, entonces, la actuación del agente encubierto, aquéllos que cometen un ilícito tienen que haber estado previamente determinados a hacerlo.

> Claro está que en algunos casos estos límites pueden ser borrosos, en especial, cuando los intervinientes todavía no están decididos a la comisión del hecho antijurídico, y el agente encubierto aparece como un factor de motivación ulterior. Por ello, deberá al menos exigirse que los involucrados hayan alcanzado la calidad de sospechosos en una fase de investigación temprana, por ejemplo, cuando exista una denuncia de terceros sobre la actividad criminal o la autoridad pública tenga sospechas razonables de la posible comisión de un delito (Aboso, 2023, pág. 401) .

Existe otra limitación a la actuación del agente encubierto, la cual está prevista en la referida Ley 27.319, y es precisamente el ya aludido sistema del numerus clausus de delitos alcanzados en que podría ser utilizada esta figura.

En su artículo 1° se indica que “La presente ley tiene por objeto brindar a las fuerzas policiales y de seguridad, al Ministerio Público Fiscal y al Poder Judicial las herramientas y facultades necesarias para ser aplicadas a la investigación, prevención y lucha de los delitos complejos, regulando las figuras del agente encubierto, el agente revelador, el informante, la entrega vigilada y prórroga de jurisdicción.

Su aplicación deberá regirse por principios de necesidad, razonabilidad y proporcionalidad.

La presente ley es de orden público y complementaria de las disposiciones del Código Penal de la Nación (Infoleg, 2024) .

En tanto que en el artículo segundo se prevé que las técnicas especiales de investigación serán procedentes en los siguientes casos:

a) Delitos de producción, tráfico, transporte, siembra, almacenamiento y comercialización de estupefacientes, precursores químicos o materias primas para su producción o fabricación previstos en la ley 23.737 o la que en el futuro la reemplace, y la organización y financiación de dichos delitos;

b) Delitos previstos en la sección XII, título I del Código Aduanero;

c) Todos los casos en que sea aplicable el artículo 41 quinquies del Código Penal;

d) Delitos previstos en los artículos 125, 125 bis, 126, 127 y 128 del Código Penal;

e) Delitos previstos en los artículos 142 bis, 142 ter y 170 del Código Penal;

f) Delitos previstos en los artículos 145 bis y ter del Código Penal;

g) Delitos cometidos por asociaciones ilícitas en los términos de los artículos 210 y 210 bis del Código Penal;

h) Delitos previstos en el libro segundo, título XIII del Código Penal.

Finalmente, la normativa define al Agente Encubierto de la siguiente manera: “ARTÍCULO 3º. Será considerado agente encubierto todo aquel funcionario de las fuerzas de seguridad autorizado, altamente calificado, que presta su consentimiento y ocultando su identidad, se infiltra o introduce en las organizaciones criminales o asociaciones delictivas, con

el fin de identificar o detener a los autores, partícipes o encubridores, de impedir la consumación de un delito, o para reunir información y elementos de prueba necesarios para la investigación, con autorización judicial (Infoleg, 2024)".

Así, un requisito insoslayable para la intervención del agente encubierto es que su designación lo sea en el marco de la investigación de alguno de los ilícitos ut supra mencionados.

Además, debe contar con expresa autorización judicial y previa solicitud Fiscal. Está totalmente prohibida su actuación sin dicha autorización, o fuera del marco de un proceso penal.

"De esa manera, se procura controlar judicialmente el accionar de los agentes encubiertos para evitar una actuación arbitraria (Aboso, 2023, pág. 404)".

En Argentina – a diferencia de España – aún no existe una regulación específica del agente encubierto online. Así es que los autores individualizan ciertas problemáticas que pueden suscitarse de su actuación en el ciberespacio.

En primer lugar, hemos visto ya el sistema de numerus clausus de delitos para los cuales se puede echar mano de esta figura. Si bien es cierto que los delitos mas comunes van a estar aquí incluidos (distribución de M.A.S.I del art. 128 del Código penal, o el delito de ciber yihadismo previsto en el art. 41 quinquies del C.P., quedarían fuera otras figuras tales como el Grooming del art. 131 CP, las estafas informáticas del art. 173 inc 16 del C.P., y los daños informáticos contra infraestructuras críticas del art. 184 inc 6 del C.P.

Por otro lado, del texto de la ley 27319 pareciera entenderse que la figura en cuestión es aplicable en caso de delitos complejos relacionados con grupos u organizaciones criminales.

En efecto, en la Exposición de Motivos de dicha ley se señaló que la finalidad de la misma era hacer frente a "el auge y la evolución del crimen organizado y sus crecientes vínculos con el terrorismo internacional" (Exposición de Motivos, Ley 27319).

Aquí conviene poner de resalto que no todo delito informático puede ser encuadrado en el concepto de "complejo" o relacionado con "grupos u organizaciones criminales" (Salt & Polansky, 2023).

Es que son variadas las actividades ilícitas que se llevan a cabo por internet que son cometidas por una sola persona, con lo cual no encuadrarían en esta categoría, como sucedería con el delito de Grooming del art. 131 del C.P.. Si así lo entendemos, nos quedaríamos sin la posibilidad de recurrir a esta útil figura investigativa para estos casos.

Sabemos que es precisa la autorización judicial para que pueda intervenir un agente encubierto on line. Ahora bien, nos preguntamos el motivo, puesto que, si partimos de la base que el agente encubierto no conlleva por sí la vulneración de ninguna garantía constitucional según lo resuelto por la Corte Suprema de Justicia en "Fiscal c. Fernández", podría no entenderse tal requisito de la Ley 27.319.

Autorizada doctrina llega así a la conclusión de que el legislador argentino ha entendido “que el hecho mismo de la vulneración del principio de confianza mutua en virtud del cual el Estado no debe valerse de mecanismos engañosos para inducir al error a los ciudadanos justifica la exigencia de una preceptiva autorización judicial” (Salt & Polansky, 2023, pág. 227).

Entonces nos surge la siguiente pregunta: en caso de necesidad de afectar algún derecho fundamental adicional durante el desarrollo de la actuación del agente encubierto, ¿conlleva la necesidad de una resolución judicial adicional y/o específica? O, al contrario, si la previsión de

la Ley 27.319 en su artículo 30 ya cubre todas las posibles afectaciones de derechos adicionales que se produjeran durante su desarrollo.

Sucede que el escenario habitual con que se encontrará el agente encubierto digital es con canales cerrados donde diferentes personas - tengan o no el rótulo de investigados - mantienen conversaciones con una expectativa razonable de privacidad.

Al respecto, entiende autorizada doctrina que solamente en aquéllos casos en los que durante la investigación se afecte un derecho fundamental distinto a los que se tuvo en cuenta al momento de ser autorizada por el Juez la operación encubierta, por ejemplo, se torna menester un allanamiento de domicilio, se deberá solicitar por los canales normales la autorización para vulnerar la inviolabilidad del mismo, no resultando cubierta por la autorización primigenia. (Salt & Polansky, 2023)

3.3 Deberes del Agente Encubierto

Al ser el agente encubierto un funcionario público, encuentra su actuación enmarcada en la Ley de Ética Pública (ley 25.188), como así también registra limitaciones funcionales específicas relativas a su calidad de tal (ley 21.965).

Como vemos, el agente encubierto se encuentra en cierto modo equiparado a un testigo, ya que deberá deponer en el proceso penal, revistiendo un doble carácter: funcionario público y testigo.

Así, tendrá los mismos deberes que un testigo: comparecer, declarar y decir verdad. Caso contrario, se encontrará sujetos a las penas del testigo renuente (art. 243 del C.P.), y del falso testimonio (art. 275 del C.P.)

Claro está que resultaría lógica una petición en el sentido de preservar su integridad física, puesto que el mismo ha estado en el seno de la organización delictiva que se pretende desmantelar. Es por ello que se podrían adoptar medidas de protección tales como la incorporación por lectura de sus informes, la declaración por video conferencia de espaldas s la cámara y similares.

Lo que debe siempre asegurarse es el debido ejercicio del derecho de defensa, quien deberá poder llevar a cabo un contrainterrogatorio directo del funcionario policial que intervino como agente encubierto (Aboso, 2023).

Ello se fundamenta en el derecho de raigambre constitucional del imputado de confrontar a la prueba de cargo.

La actual forma de interacción entre las personas nos permite afirmar que existe una especie de renuncia implícita a la confidencialidad de determinados aspectos de la personalidad.

Esta renuncia que sin dudas es voluntaria, lo es a los efectos de lograr determinados fines éticos, laborales o, que determinan que en Internet se proceda al “levantamiento del velo” de determinados aspectos o datos que, aunque personales, pueden ser aprovechados por cualquiera para averiguar elementos de nuestra personalidad (Salt & Polansky, 2023).

Está claro que aquellos datos que se vinculan a la personalidad de los sujetos que ellos mismos voluntariamente abandonan o ceden voluntariamente a fin de llevar a cabo una vida pública, pueden ser utilizados por el Estado en sus investigaciones.

La famosa Sentencia del Tribunal Superior de España STS 292/2008, de 28 de mayo, donde al analizarse la legalidad de los metabuscadores de pornografía infantil en la red, señalaba: "Ahora bien, cuando la comunicación a través de la Red se establece mediante un programa P2P, como en el Emule o Edonkey, al que puede acceder cualquier usuario de

aquélla, el operador asume que muchos de los datos que incorpora a la red pasen a ser de público conocimiento para cualquier usuario de Internet, como, por ejemplo, el IP, es decir, la huella de la entrada al programa, que queda registrada siempre. Y fue este dato, el IP del acusado, el que obtuvo la Guardia Civil en su rastreo de programas de contenido pedófilo, dato que era público al haberlo introducido en la Red el propio usuario - el acusado - al utilizar el programa P2P. Por ello, no se precisa autorización judicial para conocer lo que es público, y esos datos legítimamente obtenidos por la Guardia Civil en cumplimiento de su obligación de persecución del delito y detención de los delincuentes, no se encuentran protegidos por el art. 18.3, CE"(España, 2024).

Esto es válido para el caso del agente encubierto también, en donde el Estado se vale de maquinaciones o engaños tales como creación de identidades falsas y documentación que las respalde, a fin de lograr introducir un agente en determinadas organizaciones tendientes a descubrir cómo funcionan y, en definitiva, intentar desbaratarlas.

> Para ganarse la confianza del sujeto objeto de investigación, el agente encubierto puede verse obligado no solo a interactuar y establecer una relación habitual con el investigado sino que, además, el establecimiento de dicha relación de confianza puede llevar al extremo de acceder a datos referentes a la privacidad que no sean públicamente conocidos y que, consecuentemente, no hubieran podido ser objeto de aprehensión o interceptación a través de una vigilancia o seguimiento tradicional. En definitiva. el establecimiento de una mutua relación de confianza entre el agente infiltrado y el individuo sujeto de investigación puede conllevar apriorísticamente el acceso a datos de privacidad que, lejos de pertenecer a la esfera más externa de la intimidad, suponga la intromisión en aspectos más esenciales de la privacidad. No es complicado imaginar situaciones como las descritas: el agente encubierto que, en base a una relación de confianza con el investigado, descubre sus problemas maritales, la existencia de un

> amante, sus gustos personales, el acceso a un diario o álbumes de fotos familiares, etcétera (Salt & Polansky, 2023, pág. 240).

Entiendo que un tema discutido es el relativo a la validez del ingreso del agente encubierto al domicilio del investigado. Se discute sobre si la autorización judicial inicial para que un funcionario revista la calidad de agente encubierto, habilita también la intromisión al domicilio de los sujetos investigados. Al respecto existen dos posturas.

Por un lado, Perals Calleja se han posicionado en contra de la necesidad de una resolución judicial adicional.

> "En el momento en el que el agente encubierto acepta una invitación para entrar en el domicilio del investigado no está realizando una prueba preconstituida de entrada y registro domiciliario, sino que está ejecutando las labores propias de su infiltración que, recordemos, está amparada judicialmente y que tiene una finalidad proporcional y legítima, valorada y admitida por el juez de Instrucción (...) Así, pues, la autorización judicial al agente encubierto para infiltrarse en una organización criminal valora también que van a ver afectados derechos fundamentales del investigado, entre ellos, el derecho a la intimidad que ejerce en su domicilio" (Calleja, 2010, pág. 241) .

En apoyo de esta postura se ha dicho que la autorización para engañar habilita a no revelar la identidad al investigado en ningún supuesto. Así, es perfectamente válido que el agente encubierto online oculte y/o silencie su condición, y las probanzas colectadas durante su función serán perfectamente válidas para ingresar al proceso.

Es que no podemos dejar de considerar que, en los casos que analizamos, tiene valor el propio consentimiento que ha dado el investigado; es este consentimiento lo que autoriza el ingreso al domicilio. Así, si el ingreso a la morada de éste fuera producto de una invitación del investigado, la actuación será perfectamente válida. Lo que no puede el agente encubierto hacer

– claro está – es ingresar al domicilio sin el consentimiento del morador. Para ello se requerirán las autorizaciones judiciales específicas a fin de poder vulnerar la garantía constitucional de la inviolabilidad del domicilio.

Es que “el vicio que supone el engaño es permitido por los órganos de persecución penal" (Salt & Polansky, 2023, pág. 241).

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. Nuevamente se produce un aumento de la intensidad de protección, justificada por el bien jurídico protegido en este caso, pues se admitiría incluso la grabación de imágenes en el domicilio (Fuentes, 2024).

Este compromiso de derechos no puede ser autorizado de forma mecánica en el inicio de la investigación, sin existir indicios específicos de su necesidad, para cumplir los principios mencionados anteriormente de proporcionalidad, idoneidad y excepcionalidad. La grabación de imágenes en domicilio en los supuestos de agente encubierto físico, ya han planteado problemas en el pasado, al tratarse de un consentimiento del titular del domicilio, que se encuentra viciado por el “engaño” del policía (Fuentes, 2024).

Pese a no ser un acceso con autorización plena, sí se entiende que el agente encubierto que accede al domicilio en estas circunstancias, puede declarar en el juicio oral como testigo de lo que ve y lo que oye, aunque nunca apotrar grabaciones (Fuentes, 2024).

En la vereda de enfrente se encuentra autorizada doctrina que entiende que no se encuentra autorizado al agente encubierto a ingresar al domicilio del investigado.

Es que advierten que dicha renuncia voluntaria y consentida a la privacidad se ha producido como consecuencia de un error, inducido por el propio Estado.

"El engaño no puede llegar hasta el punto de desproteger al ciudadano en la autotutela de los aspectos axiológicos y más profundos de su privacidad" (Salt & Polansky, 2023, pág. 241).

Es oportuno citar un fallo de la Corte Suprema de Justicia de la Nación de fecha 11 de diciembre de 1990, que lleva la carátula "Fiscal c/Fernández", en donde se que declaró no vulnerado el derecho a la intimidad del condenado al producirse una entrada del agente encubierto en el interior de su domicilio. En dicho caso se consideró que se había producido una ausencia de autotutela en la protección del derecho fundamental por parte del condenado al no preocuparse en saber quién era el desconocido que invitaba a entrar en su domicilio.

4 EL AGENTE ENCUBIERTO ONLINE

A aquellas investigaciones llevadas a cabo en el ciberespacio le resultan aplicables todas las consideraciones anteriormente vertidas.

Ahora bien, no podemos desconocer que el agente encubierto online va – en la realización de su tarea – más allá de la operación que se desarrolla en el mundo no virtual.

Es que cuando el Fiscal solicita y el Juez autoriza la actuación de un agente encubierto digital, está autorizando a un funcionario público a ingresar a un *canal cerrado de comunicación* donde se va a encontrar con una cantidad indeterminada de suscriptores y/o usuarios, quienes intercambian ideas, expresiones y también archivos con la razonable expectativa de tener privacidad a tal fin.

> Ello implica no solo una afectación aún mayor del derecho a la privacidad (entrando en ámbitos de la misma que podríamos denominar axiológicos), sino una directa injerencia en el derecho al secreto de comunicaciones por lo que la necesidad de una resolución

> judicial habilitante quedaría fundada en la garantía constitucional establecida directamente en el art. 18.3 de la CE.
>
> La problemática estribaría en determinar cuándo un canal de comunicación puede ser catalogado como cerrado y cuándo no. Esta cuestión no resulta ociosa. La catalogación de un canal de comunicación como cerrado o abierto constituye la auténtica clave de bóveda para determinar los límites de actuación del ciberpatrullaje y la concreción del momento exacto en la que los agentes encargados de la investigación del delito deben dejar de actuar y requerir la cobertura de una resolución judicial (Salt & Polansky, 2023, pág. 245).

A fin de determinar si un canal es abierto o cerrado no se pueden indicar a priori sus configuraciones y definir de antemano cual es o no un tipo u otro. Tendremos que ver en cada caso en particular, y en cada foro o canal de comunicación, si se reúnen determinadas características que nos permitan afirmar si estamos ante un canal abierto o cerrado.

El canal abierto puede, sin duda alguna, ser objeto de investigación y ciberpatrullaje policial sin autorización judicial previa.

Lo que está abierto para todo el mundo, lo que es público, también es público para el Estado.

Es así que cualquier probanza que se obtuviere de este tipo de canales puede ser válidamente incorporada como prueba, e incluso se podrá prescindir en estos casos de la utilización de la figura del agente encubierto digital, pues será el propio efectivo policial quien podrá verificar si se dan los extremos de una conducta ilícita.

> Son dos las características que dotan a un canal de comunicación digital de la condición de canal cerrado: I) Por un lado, la existencia de una clasificación de seguridad, elemento que debe ser interpretado de una manera flexible, atendiendo al grado de

> seguridad exigido en cada caso. No deben recibir el mismo tratamiento, por lo tanto, supuestos en los que la formalización del alta consiste en introducir un nombre y un apellido, que en casos en los que la admisión en el grupo está condicionado, por ejemplo, a recibir una invitación por parte de otro miembro del grupo, a la presentación de una documentación auténtica que acredite la verdadera identidad del nuevo miembro, o, en definitiva, a cualquier otra circunstancia que haga presuponer la existencia de medidas de seguridad más rigurosas que la mera cumplimentación de un formulario o modelo estereotipado, y ll), consecuencia de lo anterior, la existencia de una expectativa razonable y fundada de privacidad de los usuarios del citado grupo (Dupuy, 2020, pág. 246).

En el canal cerrado se elimina el carácter público de determinados contenidos que el administrador del mismo previamente elige, a los que sólo van a poder acceder las personas por él elegidas y aceptadas.

“En un canal cerrado existe una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas, exigiéndose una previa invitación para poder incorporarse al canal de comunicaciones” (Salt & Polansky, 2023, pág. 245).

En efecto, el protocolo sobre "la prevención policial del delito con el uso de fuentes digitales abiertas", dictado por la República Argentina el 26 de mayo de 2020, en su art. 20 define como canal abierto de comunicación a los medios y plataformas de información y comunicación digital de carácter público, no sensible, y sin clasificación de seguridad, cuyo acceso no implique una vulneración del derecho a la intimidad de las personas, conforme a lo normado en la Ley de Protección de Datos Personales N° 25.326 y sus normas reglamentarias.

> Ejemplo paradigmático de la dificultad de efectuar una separación entre el concepto canal privado y canal abierto se da con ocasión de las investigaciones desarrolladas en

> la red social por excelencia: Facebook. Respecto a ello, de la propia idiosincrasia de este tipo de plataformas interactivas se infiere, con meridiana sencillez, que sus usuarios no pueden tener una 'expectativa razonable de privacidad respecto a lo publicado en las mismas. En definitiva, millones de usuarios están compartiendo diariamente contenidos multimedia siendo, en la mayoría de los casos, estos contenidos fácilmente accesibles por cualquier usuario de la red. En base a ello, parece que difícilmente podría ser considerada dicha red social como 'canal cerrado' a los efectos de la realización de actividades de ciberpatrullaje. Sin embargo, esta aseveración no sería igualmente aplicable a aquellos supuestos en los que, por la propia configuración de seguridad establecida por el usuario, no fuera visible el contenido de un perfil personal para terceros no deseados (o cuando estamos hablando del contenido publicado en un foro privado dentro de la propia red social). En estos casos, sí podríamos hablar de que los usuarios afectados tendrían una expectativa razonable de privacidad respecto a lo manifestado, o publicado, en estos espacios y, consecuentemente, sí sería exigible el dictado de una resolución judicial a fin de que los agentes de las fuerzas y cuerpos de seguridad del estado pudieren monitorizar lo que ocurre en los mismos" (Salt & Polansky, 2023, pág. 246).

Para ingresar a la red social Facebook es necesario la creación de un perfil, desde el cual el usuario se logueará y podrá navegar en dicha red. Toda la actividad será pública, salvo que se configure como privada. Para poder interactuar con otras personas, se lo deberá aceptar como *amigo* en dicha red social. De este modo, aquella persona sospechosa va a autorizar o consentir la inclusión del perfil del agente investigador entre sus contactos.

Veamos un ejemplo de lo que venimos exponiendo. En una investigación ´por ciber yihadismo se utilizó, como medio de investigación, el agente encubierto online. En efecto, la Policía Nacional del Principado de Asturias detectó que en la red social Facebook, existí un perfil que por su simbología podría aparecer vinculado al entorno yihadista, puesto que la imagen de perfil era una bandera negra del DAESH. Así, se solicitó al juzgado la autorización para actuar con la modalidad de agente encubierto virtual, la cual fue otorgada y, mediante la creación de un perfil falso por parte de la autoridad, fue el propio sospechado quien envió una solicitud de amistad a las autoridades, pasando así a ser de su grupo de "amigos". Una vez obtenido tal carácter, el agente encubierto pudo acceder al perfil completo del sospechoso, y así detectar numerosos videos y fotos publicados con discursos de líderes de perfil yihadista como Abu Musab Al Zarqaui, y cánticos a favor de los mártires por la causa de Dios (Salt & Polansky, 2023).

No debemos confundir las patrullas cibernéticas con el agente encubierto informático, pues estas patrullas operan en los canales abiertos de internet, como un usuario más, pero que no precisan de una identificación y posterior autorización para entrar en un foro determinado y cerrado. Sin embargo, fruto de estas investigaciones en canales abiertos, se han producido investigaciones de agentes encubiertos, que han contactado de forma casual en un foro abierto.

Otro ejemplo que podemos traer a colación se dio en España, en donde la Guardia Civil detectó en la página web wwv.sexotabu.com, mediante la realización de ciberpatrullaje, que existía un perfil que se dedicaba al intercambio de archivos de material de abuso sexual infantil. Luego de mantener los agentes conversaciones privadas con dicho usuario, éste les comentó que existía un foro privado de nombre "La Gran Familia", en donde adultos concertaban encuentros de naturaleza sexual haciendo participar en los mismos a sus propios hijos.

Dicha red fue desactivada gracias a la utilización de la figura que venimos estudiando. Si bien la defensa realizó numerosos planteos de nulidad aduciendo que su cliente había sido engañado por el propio Estado, todos y cada uno de ellos fueron rechazados, confirmando así la legal actuación del agente encubierto online (Salt & Polansky, 2023).

4.1 Niveles en la investigación y autorización judicial

Tal como enseña la experta en Cibercrimen Daniela Dupuy, existen tres niveles en que el Estado puede actuar en el ciberespacio a fin de controlar las actividades delictivas que en él se produzcan y, dependiendo de cuál sea el nivel, es si se necesita algún tipo de autorización para actuar por parte del agente y, en su caso, qué especie de autorización.

En primer lugar, señala que el nivel N° 1 está dado por lo que se conoce con el nombre de Ciberpatrullaje, en donde señala que hay aquí un primer grado de afectación en la intimidad y/o privacidad de los usuarios. Se trata de los rastreos policiales destinados a la vigilancia, prevención y evitación de delitos en el ciberespacio, pero en particular en espacios de libre acceso o canales de comunicación abiertos, tales como redes sociales o foros de Internet.

Debemos aquí remarcar la importancia que ha adquirido en el tema en estudio lo que se conoce como Open Source Intelligence (OSINT), o análisis de fuentes abiertas. Se comprenden aquí a las herramientas, técnicas y tecnologías que permiten recolectar información que está disponible públicamente (Acosta, 2024).

Nos referimos a documentos, textos, audios, imágenes, videos. Que se encuentren disponibles públicamente implica que no es necesario contar con credenciales de seguridad como puede ser, por ejemplo, un usuario y una contraseña.

En cuanto a las redes sociales, la recolección de información en este campo constituye una práctica ya independiente de la OSINT, que los expertos denominan SOCMINT (Social Media Intelligence).

Mediante ella se puede lograr la revisión manual del contenido publicado, como así también la revisión de búsquedas específicas de usuarios, hashtags; el uso de herramientas de scraping para extraer contenido en una página web; e incluso la sistematización de las técnicas anteriores mediante distintos tipos de software (Acosta, 2024).

Estas técnicas constituyen lo que conocemos como "ciberpatrullaje". El primer antecedente data del año 2007, cuando a partir de los datos proporcionados por la plataforma pública satelital "Google Earth", el organismo fiscal de la Provincia de Buenos Aires anunciaba el entrecruzamiento de los mapas satelitales con las declaraciones impositivas, como método para investigar eventuales conductas evasivas (Acosta, 2024).

Para realizar este tipo de tareas, no se requiere autorización judicial previa, puesto que esta actividad se asemeja a la vigilancia que realiza el personal policial en la vía pública en su función preventiva.

En el segundo nivel nos encontramos ya con un agente estatal que utiliza pseudónimos para inmiscuirse en salas de chat o redes sociales. Aquí ya existe un nivel de infiltración un poco más profundo que en el caso anterior, en donde los agentes del Estado ocultan su condición con el investigado, y mediante la utilización de un usuario con un Nick determinado que no coincide son su verdadera identidad, oculta su identidad a éste, tendiente a reunir elementos probatorios para poder dar continuidad exitosa a la investigación.

En este caso tampoco se requiere de autorización judicial puesto que, en la medida en que no se vulneren garantías constitucionales, y mientras se maneje en el plano de chats

públicos y/o redes sociales de acceso público, su actuación no difiere de la actividad preventiva de la policía en su actuación en el plano físico (Dupuy, Innovaciones Digitales, 2023).

Yendo más allá, y ahora en un tercer nivel, cuando de canales de comunicación cerrados se trata, sí se requiere indefectiblemente la autorización judicial que habilite a un agente encubierto a interactuar con el investigado.

4.2 El agente encubierto y la preservación de la evidencia digital

Es de fundamental importancia señalar que el agente encubierto debe estar especialmente capacitado no sólo en utilización de redes sociales y/o chats y la terminología a utilizar con los presuntos agresores a fin de evitar ser detectado sino que, además, debe encontrarse altamente capacitado en lo que se refiere a evidencia digital.

En especial, al modo de resguardar la misma, para que pueda ser presentada en juicio y no pierda validez alguna.

Es decir, el agente encubierto online debe actuar tomando todos los recaudos para preservar esa evidencia digital que va obteniendo en el marco de su investigación, a fin de poder ulteriormente presentarlas en juicio.

Enseña la Dra. Dupuy que las conversaciones que el agente encubierto mantiene con la persona sospechosa pueden ser muy fugaces, y da el ejemplo de la aplicación Telegram, la cual puede ser configurada para que los mensajes se eliminen automáticamente tras escasos segundos, o luego de ser vistos por una única vez inclusive (Dupuy, Innovaciones Digitales, 2023).

Deberá el agente encubierto identificar desde qué dispositivo mantuvo la comunicación, señalando marca, modelo y número de serie, como así también tomar registros fílmicos de la interacción con el investigado.

Luego, esos registros fílmicos deberán ser descargados y preservados con su respectivo código Hash. Así, se podrá demostrar la identidad, preservación y registro de la prueba, como así también se va a evitar que la misma sea contaminada o alterada (Dupuy, Innovaciones Digitales, 2023),

Debemos aquí señalar el precedente “United States v. Jackson”, en donde se consideró inválida la incorporación de registros de conversaciones una sala de chat, puesto que el agente encubierto que había intervenido en ellas, lo que había hecho era “copiar y pegar” dichas conversaciones en un documento “*.doc”, es decir, ejecutable en un software al estilo de Word de Microsoft Office, en vez de presentar los registros originales o una imagen informática de aquellos.

.

4.3 Rastreo de archivos ilícitos a través de algoritmos. Uso del Hash.

La manera de identificar los archivos informáticos es a través del HASH, que consiste en una clave alfanumérica de los archivos, que es única para cada archivo. En caso de sufrir cualquier tipo de modificación el archivo, también se modificará, indefectiblemente, el Hash.

Tal identificación es de vital importancia, para conocer los recorridos y modificaciones, que se les hace, para tenerlos localizados y más aún, si estos archivos ilícitos, han que ser introducidos por el propio agente encubierto informático, para tras hacer su función, localizarlos y eliminarlos y evitar la temida provocación de delito (Fuentes, 2024).

El control y rastreo de los algoritmos, a través de la Inteligencia Artificial, permiten conocer todos los recorridos que han tenido, donde se han generado y por qué IP han pasado. La importancia de este código viene a ser fundamental a la hora de poder rastrear los movimientos y modificaciones de los archivos ilícitos intercambiados por el agente encubierto informático, con el objeto de eventualmente destruirlos.

4.4 Utilización de troyanos

En España se permite el acceso y registro de dispositivos informáticos de forma remota, mediante la instalación de software (art. 588 de la LECrim). Este software es conocido como troyano o malware, y permite acceder a todo tipo de información y datos (Fuentes, 2024).

4.5 La experiencia con Sweetie

El 21 de octubre de 2014 se conoció a través del periodismo la noticia de que una "niña virtual" había conseguido desenmascarar a un pederasta australiano tras haber mantenido conversaciones con él a través de un chat.

La niña virtual, a la que apodaron Sweetie, es un personaje creado informáticamente por la organización holandesa Terre des Hommes.

Sweetie mantuvo conversaciones online en plataformas de chat abiertas, en donde es frecuente que reciba mensajes de hombres adultos que, a medida de progresa la conversación, comienzan a exigirle a la presunta niña que realice conductas sexuales, que encienda la web cam, que envíe fotos y hasta que se masturbe frente a ellos (Iberoamericana, 2019).

Es de destacar que en sólo dos meses los investigadores localizaron a unos veinte mil pedófilos que, además, intentaron pagar por tener relaciones sexuales con la menor.

Desde Terre des Hommes se ha hecho una fuerte campaña para instar a los gobiernos a que inviertan en este tipo de herramientas para ayudar a combatir la pedofilia y la pederastia.

> Tras los buenos resultados obtenidos por Terre des Hommes con la utilización de Sweetie, consideramos que la creación de robots inteligentes sería una muy buena herramienta para combatir delitos contra menores, dado que, en primer lugar, los agentes infiltrados que operan en chats con el objetivo de localizar pedófilos tienen que soportar una fuerte carga psicológica por la exposición continuada a contenidos de pornografía infantil, por lo que han de ser sustituidos cada cierto tiempo y pueden tener secuelas psicológicas, problema que se eliminaría si fuera un robot el que tuviera que tratar con esos contenidos. Asimismo, el gasto que conlleva formar a nuevos agentes, tanto en habilidades comunicativas, como psicológicas, así como también informáticas, sería menor en caso de que se utilizaran robots que, pese a que su elevado coste de fabricación, a largo plazo serían amortizables (Iberoamericana, 2019, pág. 37/39).

Ahora bien, para no caer en un delito provocado, habría que programar el robot de manera que simplemente creara un clima de confianza en el que el pedófilo desvelara sus verdaderas intenciones delictuales, sin que fuera el propio robot el que lo instara a cometer el delito.

En este punto es necesario remarcar que el agente que utiliza este avatar debe evitar involucrarse de tal manera que hubiese creado o instigado la ofensa criminal en la cabeza del delincuente, ya que de lo contrario, su comportamiento estaría determinando la voluntad del otro, convirtiéndose en un '"agente provocador" ("Fiscal c: Fernández", CSJN),

No obstante, la sola existencia de un Avatar como el caso de Sweetie no constituye un caso de provocación o entrapment, puesto que su presencia e interacción en un chat no supone una incitación relevante si el avatar se limita a estar presente y dar conversación a terceros, sin

proponer directa o indirectamente la comisión de delito a alguna de las personas con las cuales entabla dichas conversaciones.

Ahora bien, si el avatar se utiliza para provocar la comisión de estos delitos, intentando crear la ocasión pero también yendo más allá, es decir, provocando al agresor a *seguir el juego*, dándole una oportunidad para que concrete su acción delictiva e incluso tendiendo *trampas* para que éste avance con su accionar ilícito, ahí sí podríamos estar en presencia del *agente provocador*, y por ende, correr el riesgo que sean nulificadas las actuaciones de investigación, por haber vulnerado derechos del sospechado de jerarquía constitucional.

4.6 CATT (Chat Analysis Triage Tool)

El CATT (Chat Analysis Triage Tool) es una poderosa y útil herramienta que permite investigar el online child grooming.

Cabe destacar que no todos los agresores sexuales de la red buscan el efectivo contacto sexual con los menores víctimas, sino que existen aquéllos que buscan el cibersexo y los juegos de rol.

Por otro lado, la enorme cantidad de casos de vulneración a los derechos de libertad sexual a menores en el ámbito de la web, hacen que sea necesario distribuir los recursos en aras de determinar si este agresor busca o no dicho encuentro físico.

Se ha logrado determinar mediante estudios de casos que existen importantes diferencias entre el modo de expresarse y, por ende, del lenguaje mismo entre los menores y aquellos agresores que se hacen pasar por menores.

Es así que aparece en escena esta poderosa herramienta de análisis de chats CATT, mediante la cual se analizan, clasifican, estudian y comparan los chats entre menores,

ciberdelincuentes que sí se encuentran interesados en lograr el encuentro y/o contacto físico, y aquéllos agresores virtuales que buscan satisfacer sus bajos instintos de manera virtual, es decir, a través de la web y sin buscar tal encuentro físico.

Mediante la utilización de CATT, en cuestión de segundos sus algoritmos pueden brindar una estimación del nivel de riesgo del delincuente y la probabilidad de que cometa el delito a través de un encuentro.

Sin lugar a dudas, lo que se busca con CATT y su algoritmo es priorizar las actuaciones y los recursos policiales en los casos en que el agresor pretende un encuentro físico, donde el menor va a correr mayores riesgos, de aquél que se va a realizar en el entorno virtual.

Ahora bien, no significa que no se vaya a investigar la actuación del agresor sexual virtual, sino que los recursos se utilizarán en primer medida para evitar las agresiones físicas, en tanto que a las agresiones virtuales se les asignarán otros recursos, y se las investigará de otro modo.

En España viene dando resultados muy beneficiosos para la lucha contra este flagelo, la utilización de la herramienta en cuestión.

4.7 Regulación legal del agente encubierto informático en la provincia de Mendoza

En el año 2021 ingresó al Poder Legislativo de Mendoza un proyecto de reforma del Código Procesal Penal local, elaborado por el Fiscal de Delitos Económicos de la provincia, Dr. Santiago Garay.

Recientemente el proyecto ha obtenido sanción definitiva, convirtiéndose en ley. Uno de los aspectos novedosos que trata, reformando el artículo 29 de dicho cuerpo legal, es la figura del agente encubierto online.

En los fundamentos donde solicitó su aprobación, el Dr. Garay señaló que en determinado tipo de investigaciones, sobre todo a aquéllas relacionadas con la producción o distribución de material de abuso sexual infantil, se tornaba dificultoso llegar a buen puerto, debido a que estos delincuentes actúan – como hemos visto - en grupos cerrados. No existía manera de acceder a estos contenidos si no era con una identidad falsa.

Es así que el actual artículo 29 del Código Procesal Penal de Mendoza, absolutamente novedoso, dispone: "**Actuación Encubierta... Agente encubierto Informático**: En los casos de la investigación de delitos en que resulte de utilidad la interacción del agente en entornos o plataformas digitales, se podrá autorizar por el Juez de Garantías la actuación encubierta de un agente bajo las mismas premisas anteriores. La autorización de este medio de investigación excepcional, se emitirá -por auto fundado-, en el marco de la investigación de un delito concreto de especial gravedad y siempre que existan motivos suficientes que acrediten que los datos no pueden ser obtenidos de una forma menos gravosa para los derechos de los sospechados, el éxito de la investigación este seriamente dificultado sino se recurre a este medio o en aquellos casos en que el delito se cometa a través de medios informáticos que tornen imposible otra forma de investigación. La actuación encubierta no podrá exceder de los 90 días a contar desde su autorización y prorrogable una sola vez por igual termino. En este caso, los perfiles o identidades digitales que este agente asuma serán creados bajo las recomendaciones del personal técnico idóneo del Ministerio Publico Fiscal y bajo el control directo del Fiscal de Instrucción a cargo de la investigación, quien hará constar en las actuaciones toda la información necesaria respecto a perfiles a utilizar, plataformas digitales donde se actuara, claves de acceso validadas y actividad concreta a desarrollar por el agente. 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, pero para el caso en que su actuación implique

la utilización de programas informáticos que impliquen un acceso remoto a otro dispositivo digital, deberán además cumplirse con los requisitos exigidos por el art. 220 bis del presente Código. El agente encubierto informático 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".

Entrando a realizar un análisis del artículo en cuestión, vemos que se han receptado las modalidades y recomendaciones tanto de la doctrina como de la jurisprudencia internacional relativas a la utilización de esta figura, a saber:

- Se requiere autorización judicial para utilizar la figura;
- Solo puede ser utilizada para investigar delitos en que resulte de utilidad la interacción del agente en entornos o plataformas digitales;
- Su autorización es excepcional y deberá ser fundada;
- No se puede autorizar a intervenir al mismo de manera genérica, sino que requiere la investigación de un delito concreto;
- Ese delito concreto debe ser de especial gravedad;
- Dispone un plazo de duración para dicha autorización, que no puede exceder de los 90. Sólo puede ser prorrogada una vez;
- Se autoriza al agente encubierto informático a 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;

- En caso de necesitar realizar allanamientos remotos, deberá requerirse una autorización específica para ello;
- Se dispone que el agente encubierto informático 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.

V. CONCLUSIONES

El agente encubierto informático debe hoy estar presente en la agenda de todas las legislaciones procesales modernas.

Es obligación de los Estados el luchar contra organizaciones criminales, y contra individuos particulares, que utilizan las innumerables bondades de los avances tecnológicos y de Internet para la comisión de sus delitos y, en especial, para buscar a sus víctimas.

Las Convenciones de Cooperación firmadas por la comunidad internacional en procura de combatir la ciberdelincuencia y, en especial, aquellos agresores sexuales que buscan en Internet a sus futuras víctimas, en muchos casos menores de edad, obligan a las autoridades a utilizar su ingenio y herramientas a disposición para poder estar a la altura de combatir estas poderosas organizaciones. En el caso de individuos, su anonimato y las facilidades que tienen al alcance para profundizar el mismo, tales como enmascaramiento de IPs, o la Deep Weeb, deben obligar a las autoridades a aguzar el ingenio y utilizar todas aquellas herramientas y/o institutos que tengan al alcance para que, sin violar garantía constitucional alguna, permitan

investigar, perseguir y enjuiciar a estos delincuentes. Pero, y sobre todo, prevenir este tipo de ataques antes que produzcan consecuencias irreparables en las víctimas.

Es a tal fin que propugno se utilice la antigua figura procesal del agente encubierto, utilizada ya desde hace décadas y hasta siglos, pero *aggiornada* a las circunstancias actuales y a las nuevas modalidades de delincuencia.

Es que ya no se tiene un trato directo, físico, *face to face* con el investigado, sino que en las situaciones en estudio se trata de dos personas que se encuentran posiblemente en distintos países, de las cuales muy posiblemente no se conozca la identidad del investigado, ni su locación, ni sus datos de conexión a internet, ni su sexo o edad.

Es por ello que la utilización de esta figura del agente encubierto, debidamente autorizada por la autoridad judicial, por un período determinado para su actuación y en el marco de un caso determinado, es de fundamental importancia para investigar, procesar y eventualmente llevar a juicio y obtener condenas respecto de estos agresores.

No podemos dejar de lado los avances informáticos en el área de la Inteligencia Artificial, con lo cual también se propone en este trabajo la utilización de *bots* para realizar ciberpatrullaje en redes sociales y chats abiertos, a fin de determinar la existencia de este tipo de agresores, como así también el intercambio, producción o comercialización de material de abuso sexual infantil.

Incluso yendo más allá, propongo que se utilice la Inteligencia Artificial para suplantar al clásico agente encubierto que consistía en un agente policial calificado. Ello lo fundo en que, por un lado, es evidente el ahorro de recursos si lo que se necesita es solamente un *bot* debidamente entrenado, con algoritmos específicamente configurados para ello. Pero, sobre todo, es aconsejable que sean máquinas y no humanos quienes estén expuestos de manera permanente a tratar con estos agresores sexuales, puesto que el estar en permanente contacto

con imágenes de abuso sexual infantil, muchas veces con niños de muy corta edad, como así también el *ganarse la confianza* de estos agresores mediante el envío de este tipo de material, hacen que los agentes encubiertos sufran secuelas psicológicas de envergadura, pudiendo realizar esta actividad por cortos períodos.

Así, si se utilizara la Inteligencia Artificial para ello, se podría contar con un recurso permanente para la lucha contra este flagelo.

La delincuencia se ha actualizado y se ha armado de herramientas poderosas. Los Estados no pueden quedarse en el pasado, tienen la obligación de estar a la altura para combatirlos.

BIBLIOGRAFÍA

Aboso, G. E. (2023). *Evidencia Digital en el Proceso Penal.* Buenos Aires: B de F.

Acosta, N. (18 de 05 de 2024). *Biblioteca Corte Suprema de Justicia de la Nación*. Obtenido de https://biblioteca.csjn.gov.ar/cgi-bin/koha/opac-detail.pl?biblionumber=430007

Calleja, P. (2010). *El agente encubierto. La figura del arrepentido.* Barcelona: CENDOJ.

Digital, F. (17 de marzo de 2024). *Faro Digital*. Obtenido de https://farodigital.org/masi-el-material-de-abuso-sexual-infantil/

Dupuy, D. (2020). *Cibercrimen III.* Buenos Aires: Euros.

Dupuy, D. (2023). *Innovaciones Digitales.* Hammurabi.

España, S. T. (22 de marzo de 2024). *Vlex*. Obtenido de https://vlex.es/vid/facilitacion-pornografia-infantil-internet-42922794

Fuentes, I. V. (18 de 05 de 2024). *Revista Universidad de Cádiz.* Obtenido de Revista Universidad de Cádiz: https://revistas.uca.es/index.php/rejucrim/article/view/9731

Hertler, F. (2023). *El agente encubierto y su validez en el proceso penal.* Buenos Aires: B de F.

Iberoamericana. (2019). Actualidad Jurídica Iberoamericana Nº 10 bis. *Actualidad Jurídica Iberoamericana Nº 10 bis*, 37-39.

Infoleg. (17 de marzo de 2024). *Infoleg*. Obtenido de https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/268004/norma.htm

Insua, F. S. (18 de 05 de 2024). *Repositorio Universidad de Chile.* Obtenido de El AGENTE ENCUBIERTO: ¿PELIGRO O BENEFICIO EN ESTADOS DEMOCRATICOS?: https://repositorio.uchile.cl/tesis/uchile/2008/de-sologuren_f/pdfAmont/de-sologuren_f.pdf

Pascua, F. J. (2018). *Codigo Procesal Penal de Mendoza Comentado.* Mendoza: ASC.

Salt, M., & Polansky. (2023). *La investigación penal en el entorno digital. Tomo I.* Buenos Aires: Hammurabi.