

EL AGENTE ENCUBIERTO EN INTERNET: MENTIRAS VIRTUALES PARA ALCANZAR LA JUSTICIA

FEDERICO BUENO DE MATA

Personal Investigador en Formación del área de Derecho Procesal
Universidad de Salamanca

1. Una nueva figura para lograr la justicia en la Red

Internet se ha convertido para muchas personas en uno de los mejores inventos de la historia de la Humanidad. Las posibilidades que la Red nos ofrece son ilimitadas: compramos cualquier artículo, declaramos nuestros impuestos, reservamos desde asientos para acudir a un espectáculo hasta la próxima cita para la consulta médica. Una revolución tecnológica que llega a todos los ámbitos culturales, sociales, económicos, e incluso, al sector judicial.

El nuevo proyecto de ley de aplicación de las nuevas tecnologías en la Administración de Justicia de marzo de 2011 nos hace conjeturar una impartición de justicia electrónica, un nuevo recurso que constituye un impulso de aire fresco para muchos profesionales del sector judicial y policial que libran una intensa batalla para lograr la justicia.

Para conseguir dicho fin, muchas veces estos profesionales deben combatir todo tipo de injusticias, con independencia del plano en el que se produzcan, ya sea físico o virtual. A pesar de las ventajas que nos presentan las TIC, mucha gente ha encontrado en ellas una vía novedosa y eficaz para la comisión de numerosas conductas delictivas, aprovechándose de la poca legislación que existe al respecto debido a su continua transformación y a la falta de conocimientos técnicos del legislador. De esta manera se generan los delitos tecnológicos o ciberdelitos. Un *ciberdelito* es una actividad ilícita o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático, o sus datos, el objetivo del delito.¹

Para luchar contra ellos, muchas de las figuras que se utilizan en nuestro sistema judicial deben ser actualizadas. Si acotamos esta lucha al orden jurisdiccional penal, vemos como las Fuerzas de Seguridad del Estado cobran un papel protagonista para erradicar este mal.

En muchas ocasiones, imputar determinados delitos a sus presuntos autores resulta una tarea difícil, más aún si cabe en el plano virtual, donde el anoni-

¹ MITCHSONI, URRY “Delitos y abusos en el comercio electrónico”. *The IPTS Report*, 2001, 57, págs 19-24.

mato que ofrece la red complica esta tarea aún más si cabe. Por esta razón se deben buscar medidas para remediar este problema, soluciones para dar luz a ese territorio sombrío que propicia el anonimato con el que se cubren a diario miles de ciberdelincuentes en nuestro país.

Si dejamos los análisis forenses electrónicos y las periciales informáticas a un lado, y pensamos en las acciones que pueden llevar a cabo las Fuerzas de Seguridad del Estado para erradicar este mal, podremos focalizar nuestra atención en el análisis de la figura tradicional del agente encubierto como forma de lograr una solución al respecto.

Una figura que si la trasladamos a Internet, debe obligatoriamente cambiar sus características y su *modus operandi* para adaptarlo a los entornos virtuales, pero sin hacer que pierda su esencia. Una esencia polémica y muy debatida basada en el engaño y con la que se trataría de utilizar técnicas usadas para delinquir como técnicas a su vez de investigación o combate de este tipo de delincuencia ².

Por tanto, esta solución consistiría en infiltrar a un agente en la red para que, actuando desde la clandestinidad con una identidad supuesta, aunque siempre con sujeción a la ley, arrastre y saque a la luz del anonimato de la red a estos delincuentes. Una solución de pleno auge y actualidad, siendo un tema debatido en la actividad política reciente; tanto es así que a finales del mes de marzo de 2011 el Senado ha aprobado regular la figura del agente policial encubierto en Internet en investigaciones contra la pornografía infantil y la pedofilia³.

Por todo ello la presente comunicación se centrará en analizar la adecuación de la figura del agente encubierto a los entornos virtuales, trabajo arduo al tratarse de una figura, que ha sido, como bien indica su propia terminología, un ente marcado por la opacidad, el ocultismo y con pocas referencias legales, doctrinales y jurisprudenciales.

Analizaremos su concepto y las características especiales que esta figura tendrá en Internet, su situación legal actual, notas características y modo y ámbito de actuación en el entramado virtual con sus respectivos límites.

² Vid. VELASCO NÚÑEZ, "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías" *Revista digital El Derecho*, publicado el 24/02/ 2011 en el link: http://www.elderecho.com/penal/Novedades-tecnicas-investigacion-vinculadas-tecnologias_11_237430010.html (Fecha de consulta: 4 de Marzo de 2011)

³ Vid. <http://www.tecnoupdate.com.ar/2011/03/21/espana-agentes-encubiertos-en-internet-contra-la-pedofilia/> (Fecha de consulta: 13 de Abril de 2011)

2. La figura del agente encubierto en internet

2.1 Concepto.

Si extrapolamos el concepto del agente encubierto en el terreno físico y lo llevamos al plano virtual, podríamos definir, bajo un concepto propio, al agente encubierto en Internet como un empleado o funcionario público⁴ que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la Red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la red y que causen una gran repulsa y alarma a nivel social.

Su función consistiría en la ocultación de la verdadera identidad policial, con el fin de establecer una relación de confianza que permita al agente integrarse durante un periodo de tiempo prolongado en el mundo en el que los “ciberdelincuentes” actúan con la finalidad primordial, igualmente oculta, de obtener la información necesaria para desenmascarar a los supuestos criminales.

2.2 Legislación.

La figura del agente encubierto para infiltraciones en terrenos físicos, encuentra su regulación en el art. 282 bis LECrim, gracias a una reforma de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la actividad investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves, efectuada por Ley Orgánica 5/ 1999, de 13 de enero.

El problema con el que nos topamos aquí y que nos lleva a una situación de vacío legal, es que dicho artículo establece un *numerus clausus*⁵ o enumeración tasada de delitos que impide la investigación encubierta en otros tipos delictivos existentes y llevados a cabo la criminalidad organizada, lo cual resulta muy poco operativo, preocupante y crea dificultades prácticas innecesarias.

Por todo ello, y con el avance que supone la tecnología consideramos un error realizar una lista tasada de delitos a los que hacer frente con esta figura y nos decantaríamos más por establecer aquí un sistema de *numerus apertus* basado en categorías de delitos y no en figuras concretas; por lo que estaríamos hablando siempre de “compartimentos abiertos”, para evitar de este modo clasificaciones a que queden rápidamente desfasadas.

⁴ Concretamente podrán infiltrarse: Miembros de la Policía Nacional.; miembros de la Guardia Civil y agentes de policías autonómicas si tienen competencias como Policía Judicial; con la salvedad de que éstos últimos no podrán participar en investigaciones encubiertas con implicaciones internacionales, puesto que no son funcionarios de Policía a efectos del Convenio de Schengen.

⁵ RIFÁ SOLER se cuestiona si el listado recoge *numerus apertus o clausus*, en “El agente encubierto o infiltrado en la nueva regulación de la LECrim.”, *Poder Judicial*, núm. 55, pág. 161; nosotros entendemos que es una lista cerrada y tasada.

A la espera de su inminente regulación, al no existir una previsión legal, lo que también se debería hacer unido a lo anterior sería redefinir el concepto de delincuencia organizada contenido en el art. 282.4 bis. En dicho precepto se dice que se considera 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(...)” ; para así a continuación crear la lista tasada a la que nos referimos.

En primer lugar ser debería reformular el concepto de delincuencia organizada⁶, incorporando al precepto algo relacionado con la red puesto que aquí el término “asociación” planteado en el precepto no deja de ser demasiado abstracto. Aún así, si vemos la Red como un lugar en el que convergen multitud de personas con gustos afines en páginas webs dedicadas a ello. Por lo que en estos casos relacionados con tráfico de material pornográfico de menores o la captación de menores para fines sexuales a través de *chats*, foros o redes sociales; el concepto de asociación indicado en el precepto siempre se estaría cumpliendo, al hablar de un marco de actuación que posee la posibilidad de conectar a millones de personas en un mismo sitio web.

Si a lo anterior sumamos que el número de ilícitos indicados no están todos los que resultan susceptibles de ser cometidos por organizaciones criminales, sería un buen momento de optar, en el caso que no siguiéramos el sistema de listas abiertas, por ampliar la lista, incluyendo los delitos cometidos a través de la red, para que los agentes encubiertos de esta manera pudieran actuar en operaciones contra la pederastia y el intercambio de material pornográfico, el *grooming*, y por otro lado actualizar dicha lista tasada de delitos y amoldarla a la nueva realidad tecnológica; por ejemplo, en el caso de los delitos de terrorismo, regular también el nuevo fenómeno del ciberterrorismo⁷.

2.3 Justificación

Los recursos ofrecidos por Internet suponen una zona que propicia el anonimato de muchos delincuentes, concretamente muchos de ellos se resguardan en la Red para realizar prácticas que constituyen una gran lacra para la sociedad por dañar a los menores de edad, nos estamos refiriendo aquí a las redes de pornografía infantil.

Muchos adolescentes y los jóvenes⁸, han hecho de la Red un factor de ocio y una herramienta fundamental de estudio y trabajo. Millones de jóvenes que

⁶ DELGADO GARCÍA, “El agente encubierto: técnicas de investigación. : Problemática y legislación comparada”. *Criminalidad organizada*, J.M. Bosch, Barcelona, 2001, pág. 3

⁷ Sería planteable si podría haber una ampliación del delito de corrupción de menores para incluir esta modalidad de ataques a través de Internet. El tema del ciberterrorismo lo trato en BUENO DE MATA, “Ciberterrorismo: Tratamiento penal y procesal del terrorismo del futuro”, *Segundo Libro INCIJUP*, en prensa

⁸ Según el informe del Defensor del Pueblo titulado “Protección de Menores ante la TV e Internet”, la gran mayoría de los adolescentes españoles entre 12 y 18 años están solos cuando

emplean su tiempo libre en compartir fotos y contar su día a día utilizando de escaparate cualquier red social, foro o *chat*.

El problema es que muchas veces el peligro se esconde al otro lado de la pantalla, gente que acecha y que vigila nuestros movimientos con fines criminales. En los últimos años era raro no ver una vez por semana alguna noticia en la televisión que verse sobre la detención de alguna red de pornografía infantil, pues según los datos España se ha convertido en el segundo país del mundo y primero de Europa en consumo de pornografía infantil, según han detectado nuestras Fuerzas de Seguridad⁹.

Por ello, en los últimos años, estos pederastas son cada vez más cautos a la hora de intercambiar material en la red, lo que produce que los “ciberrastros” que usa la policía se hayan quedado cortos a la hora de perseguir estas conductas. Aún así, existen nuevos programas de rastros como el “*Gnuwatch*”, una especie de “GPS” que rastrea millones de conexiones día y noche y localiza, en un mapa, dónde se esconden los pedófilos, consumidores de fotos y vídeos sexuales de niños y que lleva activo desde finales de marzo de 2011¹⁰.

Los “ciberrastros” estaban pensados para investigar intercambio de archivos en redes P2P, como *Emule*, *Kaaza* o *Elephant*, pero no cuando estos delincuentes sabedores ya de los posibles rastros, se mudan a foros restringidos. En ocasiones el único camino para encontrar a gente que crea o trafica con material pornográfico de menores de edad, es infiltrarse en dichos foros como usuario del mismo. Sitios en los que se crea una especie de club entre los asiduos al mismo, con lo que en muchas ocasiones la cosa se complica, debido a que por miedo a investigaciones policiales, estos criminales sólo admiten entre sus miembros a personas que les han proporcionado material sensible, cuestión hasta ahora prohibida por la ley española que castiga la tenencia de pornografía infantil.

navegan por la Red (76% de la muestra), y son menos de la cuarta parte (23,7%) los que lo hacen acompañados. Qué duda cabe de que la Red puede ser un espacio de riesgo para los menores porque, por una parte, les permite acceder a determinados contenidos peligrosos, y, por otra, facilita la exhibición y rápida difusión de imágenes y contenidos de su vida personal e íntima, especialmente en las redes sociales. Todo ello les puede convertir, fácilmente, en víctimas de otros usuarios. Así, no es de extrañar que tanto chicos -un 2,1%- como chicas -un 5%- digan haber sido víctimas de agresiones sexuales a través de la Red, lo que constituye unos hechos inadmisibles.

⁹ Vid. <http://www.20minutos.es/noticia/368259/0/visitas/pornografia/infantil/> (Fecha de consulta: 10 de Abril de 2011)

¹⁰ La novedad es que *Gnuwatch* localiza la ciudad en la que se encuentra el pedófilo, de forma que es mucho más fácil de identificar y detener. Además, la aplicación, desarrollada en Estados Unidos, es capaz de rastrear el *hash* (especie de número de serie único) de cada foto y vídeo. Se puede obtener más información sobre el programa en la siguiente web: <http://www.kriptopolis.org/gnuwatch> (Fecha de consulta 20 de abril de 2011).

Estas conductas de pedofilia se agravan cuando se pasa de la pedofilia (consumo de pornografía infantil) a la pederastia (abusos sexuales)¹¹.

Hoy sabemos que los pedófilos contactan con los adolescentes a través de *chats*, redes sociales o foros haciéndose pasar por alguien más joven e intentando entablar una relación de amistad, pero siempre con un fin sexual. Esta práctica se conoce como *grooming* y está contemplada en la reforma del Código Penal que entró en vigor en diciembre de 2010, la cual pretende castigar la captación de menores con fines sexuales a través de Internet así como considerar agresión sexual (aunque no haya violencia ni intimidación) aquellos actos que atenten contra la libertad e indemnidad sexual, cuando la víctima sea menor de edad.¹²

2.4 Características especiales y necesarias para ser agente encubierto en Internet.

En este sentido deberíamos moldear las características que comúnmente son atribuidas al agente encubierto, y modularlas con el fin de lograr una figura adaptada a la persecución de estos delitos.

El principal problema con el que chocamos aquí es que no existe una lista de características tasadas que daba reunir el agente encubierto, aún así Del Pozo Pérez¹³ establece una serie de veinte características, gracias a información obtenida de fuentes policiales, de las que eliminaríamos todas las relativas a la presencia física del agente, puesto que el desarrollo de las funciones del agente será únicamente por vía virtual.

Por lo tanto características relativas a su estado civil, edad, físico o apariencia no deberían ser consideradas como relevantes a la hora de otorgar el cargo, pero si se deberían mantener las cualidades psicológicas tales como: empatía, confidencialidad, discreción o la autonomía personal para la toma de decisiones adelantándose a las situaciones, incluida la habilidad para enfrentarse a problemas y resolverlos.

¹¹ Vid. Definiciones de la RAE para distinguir los términos: Pedofilia: atracción erótica o sexual que una persona adulta siente hacia niños o adolescentes. Pederasta: Hombre que comete pederastia. Pederastia: Abuso sexual cometido con niños.

¹² Artículo 183 bis. «El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo, a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño».

¹³ Vid. DEL POZO PÉREZ, "El agente encubierto como medio de investigación procesal en el ámbito de la cooperación internacional", en *Constitución Europea: aspectos históricos, administrativos y procesales*. Tórculo, Santiago de Compostela, 2006

A todas ellas se le debería sumar unos altos conocimientos informáticos, más de los adquiridos a nivel de usuario, por lo que el perfil idóneo para ser agente encubierto Internet sería el personal que integra la Brigada de Investigación Tecnológica de la Guardia Civil o del CNP.

3. Procedimiento, *modus operandi* y límites en su actuación

El procedimiento a seguir se basa en tres puntos: autorización y otorgamiento de una identidad falsa, la utilización del engaño como *modus operandi*, y la actuación dentro de lo permitido por una autorización judicial.

3.1 Requisitos previos

Antes de nada, y de acuerdo con el articulado, la investigación que van a llevar a cabo estos agentes encubiertos debe ser autorizada por el Juez de Instrucción o de manera excepcional por el Ministerio Fiscal, que lo debe poner en tal caso en conocimiento del juez de forma inmediata.

El motivo de la autorización por el Juez de instrucción competente de la infiltración de un agente de este tipo, se basa en que el transcurso de la misma se puede llevar a cabo una restricción de derechos fundamentales, con lo que se necesita una previa autorización judicial y un control por parte del juez instructor

Para llegar a acordar la infiltración en un caso concreto se deben cumplir una serie de requisitos respecto al entorno virtual donde se va a producir. En este casos serían los mismos requisitos que se dan para la infiltración en el ámbito físico: una existencia de indicios suficientes de que se pueda estar cometiendo esos delito de especial gravedad, que la medida sea idónea para perseguir ese fin, y que sea necesaria. Por supuesto, la medida a tomar debe estar suficientemente motivada amparándose en estas condiciones aquí expuestas¹⁴.

3.2 Identidad falsa

Una vez autorizada la investigación, el agente encubierto necesitará tener una identidad falsa para poder profundizar dentro de los foros o *webs* en su investigación. Esta identidad será otorgada siempre por el Ministerio del Interior.

El procedimiento en este caso sería muy sencillo a la hora de obtener esta identificación falsa, puesto que valdría una autorización con una serie de datos personales básicos, pero sin llegar a las características que se le dan al agente

¹⁴ Vid. DEL POZO PÉREZ, “El agente encubierto como medio de investigación procesal” op.cit. pág. 5

encubierto tradicional¹⁵, en cuanto a proporcionarle una dirección, línea telefónica, historia de vida, cuenta bancaria, e historial penal y policial.

En este caso, todo lo relacionado con la parte física de la infiltración del agente encubierto se eliminaría, con lo que la tarea del otorgamiento de identidad falsa quedaría reducido a trámites muy sencillos, nada equiparable con el agente encubierto que trabaja en el plano físico. No sería por tanto necesario crear un correcto mundo paralelo social creíble, por lo que el establecimiento de esta figura desde el punto de vista del coste económico no sería problemático, puesto que no supondría ningún desembolso de dinero para las arcas del Estado.

Al margen de lo anterior, el tema de la identidad falsa no debe resultar polémico, ya que para asegurar el éxito de la investigación, resulta imprescindible mantener en secreto su identidad, ello a fin de que no sea descubierto por los integrantes de la organización delictiva en la cual se infiltra y garantice el éxito de la investigación. En estos casos la colisión con el derecho fundamental a la intimidad del investigado queda justificada con la autorización judicial y a la ponderación de los intereses en juego. Si a todo esto le sumamos además el anonimato por defecto que nos da la Red, en el que una gran mayoría de usuarios se amparan, vemos como esta colisión con derechos fundamentales de la contraparte queda bastante debilitada.

3.3 El engaño como medida

Otro tema coligado a la actuación de esta figura policial es la de su forma de actuación, basada en el engaño como instrumento principal a la hora de poner en manos de la justicia a los criminales. Aquí entrarían dos valores en juego: por una parte, la licitud de los medios utilizados por un Estado de Derecho y por la otra, la eficacia para combatir un delito que tan graves daños ocasiona y tanta repulsa tiene por parte de la sociedad.

Un tema peliagudo, debido a que el Estado se vale de un medio inmoral en la represión de un delito, a través de una figura que utiliza como medio para cumplir su función el engaño en un primer momento, y la traición a los criminales investigados *a posteriori*.

La justificación del engaño usado por el agente encubierto radica en una cuestión de política criminal¹⁶, que llega a justificar las consecuencias desvaliosas que su utilización implica. La solución viene dada por una ponderación de valores, en el que se acaba por dar preponderancia al valor “eficacia”, en el

¹⁵ Cfr. DEL POZO PÉREZ, “El agente encubierto como medio de investigación procesal ” op.cit. pág. 7

¹⁶ DELGADO MARTÍN, “La criminalidad organizada” en *Comentarios a la LO 5/99, de 13 de enero, de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilícito de drogas y otras actividades ilícitas grave*, Barcelona, Bosch, 2001, págs 4 y ss.

sentido que si se quiere luchar eficazmente contra este delito tan oculto, la mejor manera y la opción idónea es infiltrar a la persona de esta manera para llegar a una situación más favorable para la sociedad. Estamos eligiendo así una solución que reporta más seguridad y bienestar al conjunto de la sociedad y que logra la justicia, objetivo capital en un Estado de Derecho.

Sin embargo, debemos matizar que no puede existir un engaño a cualquier precio, por lo que se deben tener siempre presentes los principios de necesidad y proporcionalidad, siempre respetando los principios y las garantías procesales y los Derechos Fundamentales de cualquier persona, incluso los de los presuntos autores.

3.4 *Modus operandi* y límites

En primer lugar, lo que iniciaría la infiltración en este caso sería con la creación de un perfil falso con el que acceder al foro. Todas las informaciones personales que tenga que rellenar en los campos necesarios para autenticar dicho perfil serán los proporcionados por el Ministerio del Interior para que así se pueda llevar un control externo de la figura del agente encubierto en la Red.

Sería conveniente que para atraer la atención de los pederastas eligiera un *nickname* o apodo que se pueda familiarizar a los ojos de un tercero con alguien que simpatice o que sea afín a practicar dichos ciberdelitos. Ese puede ser un gran efecto llamada a la hora de empezar a mantener una conversación a través de los foros con estas personas.

El problema es que en muchas ocasiones los propios pederastas no se fían de la gente con la que hablan y piden algo con el fin de creer que están hablando con alguien con los mismos gustos que ellos. En este preciso momento es cuando nos topamos con un límite legal importante, puesto que la ley impide que los agentes encubiertos puedan distribuir ellos mismos videos o fotos de contenido pedófilo para intentar congraciarse con sus interlocutores.

Se ha propuesto intercambiar material pornográfico de antiguas redadas¹⁷, cuestión que no compartimos al defender siempre actuaciones que no impliquen a menores en todo el procedimiento, ya que creemos que, por encima de toda investigación criminal está la protección de la infancia.

En este caso nos decantaríamos por permitir intercambiar “material camuflado”, con esto nos estamos refiriendo a el intercambio de material pornográfico en el que aparezcan actores y actrices porno mayores de edad haciéndose pasar por menores de edad. En estos casos resulta complicado saber si

¹⁷ Vid. Artículo electrónico “Un GPS para encontrar pedófilos” en diferentes webs como <http://www.internetsano.do/index.php/news/46/54/Un-GPS-para-buscar-pedofilos-nueva-arma-contra-la-pornografia-infantil> (Fecha de consulta: 17 de Abril de 2011)

con este uso de material pornográfico, aunque sea simulado, no se estaría vulnerando realmente justo a lo que se quiere proteger, los valores y la imagen no corrompida de la infancia. Pensamos aquí, que si existe una autorización judicial que lo permita, no estaríamos vulnerando la imagen de ningún menor ni de la infancia en su conjunto, debido a que sería material específicamente creado para luchar contra este fin, y en él no se estarían involucrando en ningún momento a personas menores de edad.

El problema más grave es la posibilidad de que esas imágenes acaben siendo redistribuidas en la red en un sin fin de ocasiones, lo que provocaría tener que ir rehaciendo más material de este tipo con el fin de seguir manteniendo la confianza de los presuntos delincuentes. Un posible remedio sería intentar poner algún filtro para que esas imágenes no se pudieran redistribuir o enviar desde un ordenador que no fuera propiedad de las Fuerzas y Cuerpos de Seguridad del Estado.

Con esta solución sería discutible también lo apuntado por el inspector jefe de la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional, Enrique Rodríguez, que insiste en que una de las dificultades para acceder a las páginas pedófilas es que es necesario primero aportar material pornográfico, lo cual puede llevar a una acusación de inducción al delito al propio agente¹⁸.

La polémica entre fijar el límite que separa al agente encubierto y al agente provocador no es nueva¹⁹. En estos casos pensamos que no se actuaría como un agente provocador, puesto que en lo que se basa la figura del agente provocador es el la de inducir a realizar una determinada acción ilícita a alguien no tenía la intención de hacerlo, como bien se expone en la STS de 14 de julio de 2000²⁰, por delito provocado «se entiende aquel que llega a realizarse en virtud de la inducción engañosa de una determinada persona, generalmente miembro de las Fuerzas de Seguridad que, deseando la detención de sospechosos, incita a perpetrar la infracción a quien no tenía previamente tal propósito, originando así el nacimiento de una voluntad criminal en supuesto concreto, delito que de no ser por tal provocación no se hubiere producido aunque de otro lado su compleja ejecución resulte prácticamente imposible por la prevista intervención ab initio de la fuerza policial».

¹⁸ LÓPEZ GARCÍA, “Agente encubierto y agente provocador, ¿dos figuras incompatibles?” *Revista La Ley*, año XXIV núm. 5822. viernes, 11 de julio de 2003, pág. 2.

¹⁹ Ciertamente la expresión agente provocador posee un fundamento anterior al jurisprudencial, enmarcado en la lucha política. La literatura jurídico penal lo recoge en la primera mitad del siglo XIX para significar la actuación de quien promueve la consumación de una acción, o bien pone los medios, o crea la situación de hecho propicia que impulsa a un tercero a ejecutarla, con la finalidad de evidenciar conductas contrarias al orden establecido (es el *agent provocateur* que nace en la Francia del Antiguo Régimen y que se generaliza en el régimen del Terror del Comité de Salud Pública de Robespierre). Es el núcleo de lo que se denominó estrategia de la tensión o acción directa de la lucha política.

²⁰ STS de 14 de julio de 2000

Al existir una relación previa con el investigado y comprobar como ya ha realizado consumaciones de delitos de tráfico de pornografía infantil, el hecho de enviarles imágenes camufladas no originaría en el delincuente ese nacimiento de una voluntad criminal ante esos hechos, puesto que se constata que dicha voluntad ha existido previamente con independencia a la infiltración del agente.

4. Reflexiones acerca de la idoneidad de aceptar la figura del agente encubierto en internet

En el mundo globalizado e interconectado en el que vivimos, la sociedad está sometida a grandes peligros a los que un Estado de Derecho tiene que poner remedio. Las personas que se asocian a través de Internet con fines delictivos configuran una gran amenaza para nuestra sociedad, y más cuando el ataque es dirigido a personas especialmente vulnerables como los menores de edad, por ello hay que tomar medidas contundentes y eficaces para luchar contra esta lacra social.

La figura de infiltrar a un funcionario de las Fuerzas de Seguridad del Estado en un entorno virtual para luchar contra estos crímenes es una medida controvertida que justifica el fin por el que es creado. La polémica del engaño y del uso de actuaciones irregulares pero autorizadas judicialmente son cuestiones que al ponderarse con los beneficios obtenidos con la puesta en práctica de esta figura quedan completamente empañadas.

Al mismo tiempo la infiltración en Internet supone unos beneficios respecto a la infiltración en un entorno físico. Los trámites se agilizan al no tener que fabricar un mundo irreal paralelo a la personalidad falsa otorgada, lo que repercute directamente sobre los costes que para el Estado supone esta figura, ya que estaríamos hablando de la infiltración cercana al coste cero, debido a que lo único que se necesita para que se despliegue la efectividad del agente encubierto en internet es un equipo informático actualizado, una conexión a Internet y a un funcionario de las fuerzas de seguridad del Estado al que se le asigne tal cometido.

Siguiendo con las ventajas, vemos como las características idóneas para tener el perfil de este tipo de agente se aminorarían respecto a la infiltración en un entorno real, puesto que se eliminan todas las cualidades físicas que se exigen en los casos ordinarios y se potencia únicamente el poseer un buen conocimiento y manejo de los sistemas informáticos.

También habría ventajas para la investigación en su conjunto, ya que siempre se aseguraría la integridad y la vida del funcionario encubierto, con lo que se sabe que la investigación siempre concluiría y no habría posibilidad de que el agente cambiara de bando. Todo ello sumado a la propia agilización de la investigación al ayudarse de medios informáticos y siempre estaría sujeta a una

valoración inmediata por parte del juez instructor o el Ministerio Fiscal en su caso, con lo que cumpliríamos con lo que la ley dice al respecto de que la información obtenida sería puesta a la mayor brevedad posible en conocimiento de quién la autorizó.²¹

Sobre el *modus operandi* que tendría que llevar el agente encubierto para ganarse la confianza nos posicionamos a favor de una actuación basada en el engaño dentro del margen que la autorización judicial otorgue y siempre sujeto a los principios de necesidad y proporcionalidad, usando para ello el dialogo y el intercambio de imágenes camufladas con actores y actrices mayores de edad con el fin de no atentar contra la infancia de ningún modo.

Por último, pensamos que existen cosas mejorables respecto a la regulación de esta figura como la reforma tanto del concepto de delincuencia organizada como de la lista de delitos tasados, para adaptarlos a la nueva realidad tecnológica y porque se dejan fuera delitos característicos de la criminalidad organizada.

También debería incluirse en la regulación la forma de comparecencia del agente infiltrado en internet en sede judicial, para que no se cometan las mismas inseguridad con su homólogo en terreno físico, puesto que vemos contra su seguridad personal el hecho de que se obligue al agente encubierto a comparecer en juicio, descubriendo su identidad de forma menos segura que en el ordenamiento alemán en que, por ejemplo, comparece en juicio el superior jerárquico del agente como testigo de referencia, que cuenta lo que le ha informado su subordinado²².

Por todo ello, pensamos que la figura del agente encubierto es una solución acertada en la lucha contra estas conductas criminales llevadas a cabo en Internet por estos criminales. Depositando la fe en el buen hacer de las Fuerzas y Cuerpos de Seguridad del Estado, estamos seguro que en un tiempo no muy tardío se podrá lograr la justicia en el mundo del ciberespacio.

²¹ Apoyada por QUINTANAR DÍEZ, “El agente encubierto” en *Revista electrónica de Derecho*, núm. 1, pág. 5

²² MARTÍNEZ DE SALINAS, “Delincuencia organizada. Instrumentos Internos”, en *Diario La Razón*, de 14/10/2002, Tribunal, pág. 4.