EL AGENTE ENCUBIERTO COMO INSTRUMENTO DE LUCHA CONTRA LA PORNOGRAFÍA INFANTIL EN INTERNET

EL GUARDIÁN AL OTRO LADO DEL ESPEJO

SARA CAROU GARCÍA

DOCTORA DE LA UNIVERSIDAD DE A CORUÑA

RESUMEN

El presente artículo analiza, desde una perspectiva jurídica, la figura del agente encubierto informático, como medio de investigación del delito de distribución de pornografía infantil en Internet. En la primera parte del texto, se efectúa un estudio crítico de la figura delictiva de distribución de material pedófilo a través de medios informáticos, en el que se incluyen una serie de propuestas de reforma legislativa para ampliar el ámbito de aplicación del delito. En la segunda parte, se aborda la figura del agente encubierto informático, proponiendo ciertas modificaciones legales, que doten de una mayor flexibilidad al procedimiento de autorización de este tipo de investigación.

Palabras clave: Internet, Derecho penal, pornografía infantil, agente encubierto.

ABSTRACT

This article discusses, from a legal perspective, the figure of the undercover agent as a way of investigating the offence of distribution of child pornography in Internet. The first part of the text is a critical study of this crime, including a series of proposals for legal reform aimed to expand the scope of the offence. In the second part, we discuss the figure of the undercover agent as well as some proposed legal amendments that could allow a greater flexibility in the approval process of this type of criminal investigation procedure.

Keywords: Internet, criminal law, child pornography, undercover agent.

1. LA PORNOGRAFÍA INFANTIL EN INTERNET

1.1. INTERNET COMO ELEMENTO FAVORECEDOR DEL DELITO

La irrupción de Internet en nuestras vidas ha supuesto un punto de inflexión en la evolución social. Nuestros modos de trabajar, de comprar o de relacionarnos se han ido transformando –y continúan haciéndolo- a la par que la denominada *red de redes*, así como las aplicaciones informáticas vinculadas a la misma se van expandiendo. No cabe duda que estos avances tecnológicos nos reportan múltiples beneficios. Internet nos permite el acceso a una cantidad ingente de información y de servicios, en un corto lapso temporal, lo que nos facilita de modo notable todas nuestras actividades, bien sean domésticas, laborales o de relación interpersonal.

Estos efectos positivos del desarrollo tecnológico no son los únicos predicables de este fenómeno. La esfera delincuencial no es refractaria a las nuevas posibilidades abiertas en el universo virtual. Las oportunidades criminales se ven aumentadas, exponencialmente, en el ciberespacio. La eliminación de las fronteras físicas y cronológicas, el aumento constante de las posibilidades conectivas entre personas, junto con el pretendido anonimato del que gozan los internautas, dotan al mundo virtual de unas características inmejorables para la comisión de diversos tipos delictivos. Una de las tipologías criminales que más se ha visto favorecida, por este uso instrumental de las nuevas tecnologías, ha sido la distribución de pornografía infantil. Los pedófilos de todo el mundo han hecho de Internet el mejor medio de comunicación y ensalzamiento de sus execrables prácticas. Actualmente, las principales vías de intercambio y distribución de imágenes de abusos y agresiones sexuales a menores se encuentran en páginas web, comunidades o grupos cerrados de usuarios, chats, foros y redes *peer to peer* (Salom, 2007; Negredo y Herrero, 2016; Valverde, 2015).

1.2. LA INEFICACIA DE LOS MECANISMOS JURÍDICOS TRADICIONALES

Las peculiares características de la ciberdelincuencia, heredadas del escenario virtual en el que esta se desarrolla, hacen necesario un replanteamiento del Derecho penal tal y como lo conocemos. La relativización de los conceptos tiempo y lugar, así como la gran capacidad de mutación, propias de la criminalidad en Internet, sitúan a la clásica legislación criminal ante un reto nunca antes imaginado. El ordenamiento penal fue diseñado para sancionar y combatir una delincuencia física, en la que las posibilidades de ejecución de los actos ilícitos y el campo de actuación de los infractores eran limitados (García, 2015; Cruz, 2006). En consecuencia, la tipificación de las conductas y los medios de investigación destinados al descubrimiento de las mismas aparecen caracterizados por un alto grado de rigidez. Urge, por tanto, una reformulación del arquetipo punitivo. No se trata, en ningún caso, de renunciar a los principios penales básicos –como el de legalidad o el de seguridad jurídica- que tanto tiempo ha costado conquistar. Es cuestión de dotar a nuestro ordenamiento penal de las herramientas óptimas que, bajo la premisa irrenunciable del respeto a los derechos fundamentales, le permitan hacer frente a esta nueva realidad criminal. Para ello será necesario que ciertos delitos –como el caso de la pornografía infantil en Internet- presenten un carácter más abierto. De este modo, la ley podrá abarcar las distintas formas de ejecución del delito que se vayan sucediendo -al socaire de la evolución tecnológica- sin necesidad de esperar a las oportunas modificaciones legislativas, caracterizadas por una excesiva duración temporal. De igual modo, los medios de investigación criminal y los procedimientos que los autorizan deberán poseer un alto grado de contemporización, acorde con el vertiginoso ritmo que impera en el universo virtual.

En los siguientes epígrafes pasaremos a analizar estas dos últimas cuestiones –referidas a la ductilidad de los tipos delictivos y de los medios de investigación- en relación con la distribución de pornografía infantil en Internet y la figura del agente encubierto informático.

1.3. EL ARTÍCULO 189 DEL CÓDIGO PENAL ESPAÑOL

La distribución de material de contenido pedófilo se encuentra sancionada en el artículo 189.1 b) de la Ley Orgánica 10/1995, de 23 de noviembre (BOE nº 281, de 24 de noviembre

de 1995) (en adelante CP). En el citado precepto se castigan la producción, venta, distribución, exhibición u ofrecimiento de pornografía infantil, así como la facilitación de las citadas conductas. Como complemento de los citados comportamientos -y con el objetivo de penar a todos los actores que participan en la cadena de suministro de pornografía infantil- el apartado 5 del artículo 189 tipifica la adquisición o posesión, para uso propio, de ese tipo de material[1], así como el acceso al mismo a sabiendas, a través de tecnologías de la información o de la comunicación. El texto es fruto de la reforma operada en nuestra ley penal, a través de la Ley Orgánica 1/2015, de 30 marzo (BOE nº 77, de 31 de marzo de 2015).

El bien jurídico tutelado por la norma es de carácter abstracto y plurisubjetivo, concretándose en la protección de la seguridad y dignidad de la infancia. Se intenta proteger a los menores del peligro inherente al fomento de la pedofilia[2]. Conviene recordar que el consumo y la distribución de material pedófilo implican: a) la comisión previa de abusos y agresiones sexuales sobre menores, que son recogidos en diversos tipos de soportes; b) la estimulación de la comisión de esos delitos sexuales, para satisfacer la demanda de ese material. Los pedófilos que acceden a pornografía infantil en Internet tienden a desarrollar un afán coleccionista, a veces de carácter compulsivo, de esa clase de archivos (Jiménez, 2012; Negredo y Herrero, 2016), de modo que su incesante necesidad de acopio lleva aparejado un aumento proporcional de la oferta. Al hilo de esta cuestión, resulta obligado traer a colación que la sanción penal de la tenencia de material pornográfico infantil, destinado a una utilización privada -ya recogida en la anterior versión del CP- ha suscitado un arduo debate a nivel doctrinal. Por mi parte, defiendo la necesidad de la tipificación de la posesión de documentos o archivos pedófilos para uso propio. El consumo de pornografía infantil estimula la producción de ese material y la consiguiente explotación sexual de menores (Lemineur, 2006; Roxin, 2013; García, 2004) El pedófilo que en el interior de su domicilio se deleita con el visionado de ese tipo de imágenes, es plenamente conocedor de que está asistiendo a la violación, tortura y abuso de niños y niñas. Con su consumo retroalimenta y apoya la espiral de violencia sexual sobre los menores.

Una de las principales novedades introducidas en el artículo 189.1 b del CP es la incorporación de un concepto de pornografía infantil, entendiendo por tal la representación visual de un menor, o de una persona que aparente serlo, participando en una conducta sexualmente explícita –real o simulada-, así como la representación de sus órganos sexuales con fines principalmente libidinosos. Esta noción incluye las denominadas pornografía virtual y pornografía técnica. Según la Circular 2/2015, de 19 junio, de la Fiscalía General del Estado (en adelante FGE), la primera es aquella en la que la imagen del menor "es una creación artificial pero realista, generada a través del ordenador u otro medio". La segunda, puede definirse como aquellas imágenes en las que "aparecen personas presentadas como menores en un contexto sexual". La inclusión de estas nuevas modalidades de pornografía infantil suponen un paso adelante en la adaptación del legislador penal a las nuevas formas que puede adoptar el material pedófilo. No obstante, la pornografía infantil descrita en el CP presenta, a mi juicio, una excesiva rigidez conceptual, dejando fuera del campo de acción del reproche penal cierto tipo de material, igualmente empleado por los pedófilos para satisfacer su parafilia. En primer lugar, la norma penal exige que el material pornográfico sea visual, de tal modo que no

1 Un resumen de los argumentos empleados por los defensores y los detractores de la tipificación de esta conducta puede verse en Guisado (2007).

2 Vid. Sentencia del Tribunal Supremo (en adelante STS), Sala de lo Penal, Sección 1ª, 767/2007, de 03 de octubre, RJ 2007\7297, MP: José Ramón Soriano Soriano, FJ.1.

se reputará pornografía infantil, a estos efectos, los audios o los escritos que recojan abusos o agresiones sexuales a menores, aunque estos sean empleados con fines lascivos por los pedófilos. En segundo lugar, el concepto impuesto en el artículo 189.1 b del CP requiere que la conducta sexual en la que se ve inmerso el menor sea explícita. Al respecto, la Circular 2/2015 de la FGE, remite a los informes explicativos del *Convenio sobre la Ciberdelincuencia*[3] y del *Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual*[4]. Conforme a los citados informes, las conductas sexualmente explícitas deben abarcar, al menos, los siguientes actos reales o simulados: a) relaciones sexuales, incluyendo genital-genital, oral-genital, anal-genital u oral-anal entre menores o entre un adulto y un menor, del mismo o de distintos sexos; b) bestialismo; c) masturbación; d) abusos sádicos o masoquistas en un contexto sexual; e) exhibición lasciva de genitales o del área púbica de un niño. Olvida el legislador que los pedófilos no siempre recurren a material de contenido sexual explícito. En ocasiones estos delincuentes también emplean material aparentemente desprovisto de toda connotación libidinosa (Jenkins, 2001; Lemineur, 2006; Taylor y Quayle, 2003). Piénsese, por ejemplo, en los catálogos de ropa de baño infantil o en las fotos de menores captadas en un entorno naturista.

Por todo lo anterior resulta contraproducente, en aras a la protección de la dignidad e indemnidad sexual de la infancia, la incorporación de un concepto formal de pornografía infantil en el CP. La atribución de un carácter pornográfico depende de criterios culturales y sociales, es decir, de reglas en esencia variables. Así lo estima nuestro TS al afirmar, en la STS, Sala de lo Penal, Sección 1ª, 1058/2006, de 2 de noviembre, (RJ 2006\8165, MP: Juan Ramón Berdugo y Gómez de la Torre) entre otras resoluciones, lo siguiente:

> *la jurisprudencia ha sido reacia a descripciones semánticas sobre esta cuestión, sin duda por entender que el concepto de pornografía está en función de las costumbres y pensamiento social, distinto en cada época, cambiante, y conectado con los usos sociales de cada momento histórico (FJ 5).*

Al mismo tiempo, la pornografía posee un componente subjetivo, radicado en la mente del espectador. Una misma imagen, objetivamente desprovista de cualquier connotación sexual, puede ser susceptible, a la vez, de dejar indiferentes a unos individuos y de activar las pulsiones de otros sujetos, en función de los mecanismos psicológicos de percepción de unos y otros. En consecuencia, es imposible ofrecer una definición de pornografía infantil válida para cualquier tiempo y supuesto. Debiera ser el aplicador del Derecho -no el legislador- el que apreciase el carácter pornográfico de cualquier tipo de material, en atención al uso que se está haciendo del mismo[5].

3 Convenio sobre la Ciberdelincuencia, firmado en Budapest el 23 de noviembre de 2001. Instrumento de ratificación por España publicado en BOE nº 226, de 17 de septiembre de 2010.

4 Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, firmado el 25 de octubre de 2007 en Lanzarote. Instrumento de ratificación por España publicado en BOE nº 274, de 12 de noviembre de 2010.

5 En esta línea puede verse la STS, Sala de lo Penal, Sección 1ª, 782/2007, de 3 octubre (RJ 2007\6289, MP: Miguel Colmenero Menéndez de Luarca): "Es cierto que, tal como alega, un desnudo de una persona menor de edad no adquiere por sí mismo carácter pornográfico. Sin embargo, en el caso no se examinan esas fotos aisladas de otras o desvinculadas de una conducta relevante, sino que el Tribunal tiene en cuenta que se enfocaban principalmente los genitales de los menores, lo cual, unido a la posesión del resto del material ocupado en poder del recurrente y a los datos que demuestran la gestión de páginas pornográficas conteniendo imágenes de menores, permite inferir razonablemente que lo grabado se uniría de alguna forma a aquellas otras imágenes, lo que permite atribuirle el mismo carácter. (FJ. 2)".

2. EL AGENTE ENCUBIERTO INFORMÁTICO

La estructura tecnológica, creada para la distribución e intercambio de material pedófilo en Internet, se ha ido modificando bajo la premisa de eludir la persecución policial de estas actividades delictivas. En un primer momento, el punto de encuentro de los consumidores de pornografía infantil se ubicaba en webs específicas, no especialmente ocultas dentro del universo virtual. La lucha de las Fuerzas y Cuerpos de Seguridad contra este tipo de criminalidad obligó a realojar los canales de distribución en otros lugares de Internet, dotados de mayores restricciones de acceso (Jiménez, 2012). Pese a que actualmente continúa existiendo el intercambio a través de redes *peer to peer*, se constata una imparable proliferación de la difusión mediante grupos cerrados de usuarios, a los que no resulta fácil acceder. En ellos los pedófilos establecen relaciones estables entre sí, al mismo tiempo que retroalimentan y autojustifican sus conductas parafílicas (Valverde, 2015; Ruiloba, 2006; Salom, 2009). Este traslado de los centros de distribución de pornografía infantil hacia la conocida como *Deep Web* provoca que las técnicas de investigación policial, como el ciberpatrullaje –cuyo ámbito de actuación natural se sitúa en los lugares abiertos de Internet-, se tornen infructuosas. No obstante, como se verá a continuación, esa frontera infranqueable para los ciberrastreos puede ser ultrapasada por el agente encubierto informático.

La incorporación de la figura del agente encubierto informático al ordenamiento procesal español se produce mediante la modificación operada en el Real Decreto de 14 de septiembre de 1882, aprobatorio de la *Ley de Enjuiciamiento Criminal* (Gaceta de 17 de septiembre de 1882) (en adelante LECrim), a través de la Ley Orgánica 13/2015, de 5 de octubre, de *modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica* (BOE nº 239, de 6 de octubre de 2015). Aparece regulado en el apartado 6 del artículo 282 bis del citado texto procesal[6]. Se configura como una técnica de investigación, empleada por la Policía Judicial, que presenta una naturaleza jurídica, a medio camino, entre la infiltración policial física y la intervención de comunicaciones telemáticas. El agente encubierto informático puede ser definido tal y como señala Zaragoza (2017) como aquel:

> *miembro de las Fuerzas y Cuerpos de Seguridad del Estado que, voluntariamente, y mediando la correspondiente resolución judicial, se infiltra en la Red con el fin de obtener información sobre prácticas delictivas producidas a través de la misma y la identificación de sus autores y/o partícipes (p.2).*

El agente infiltrado opera en la Red bajo una identidad falsa, lo cual le permite adentrarse en los grupos cerrados de pedófilos, generando para ello una relación de confianza con alguno o algunos de sus miembros, que serán los que le proporcionen la indispensable invitación para formar parte de esas comunidades virtuales delictivas.

6 Vid. artículo 282 bis 6 de la LECrim: El Juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a. El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.

2.1. LOS DELITOS PERSEGUIBLES POR EL AGENTE ENCUBIERTO INFORMÁTICO

Según el tenor literal del artículo 282 bis 6 de la LECrim, la infiltración *on line* tendrá por objeto el esclarecimiento de "alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a". Como puede observarse, el agente encubierto virtual posee un campo de actuación mucho mayor que el de su homólogo del mundo físico. Frente al *numerus clausus* instaurado en el artículo 282 bis 4 de la LECrim, el apartado 6 del citado precepto establece una lista abierta de delitos susceptibles de investigación mediante la figura de la infiltración virtual, en la que además no es exigible siempre la apreciación de delincuencia organizada. A este respecto, téngase en cuenta que el artículo 588 ter a), alude de manera explícita a "alguno de los delitos a los que se refiere el artículo 579.1 o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación". De tal modo, la distribución de pornografía infantil a través de Internet, investigada mediante operaciones encubiertas virtuales, no tiene que estar enmarcada necesariamente dentro de una criminalidad organizada, a la que alude el artículo 282.bis 4. Ello permite soslayar los problemas interpretativos, que ha generado la apreciación de la existencia de un concierto previo y una estructura jerarquizada, entre los miembros de las comunidades pedófilas en Internet. En este sentido, la STS, Sala de lo Penal, Sección1ª, 913/2006, de 20 de septiembre (RJ 2006\640, MP: José Antonio Martín Pallín) en el caso de distribución de material pedófilo en una comunidad virtual, no apreció la agravante de pertenencia a una organización criminal argumentando que:

el legislador, con vaguedad e imprecisiones, define la organización como un conjunto de tres a más malhechores y les exige una mínima estructura y coordinación. Esto supone que el concepto de organización lleva implícito un pacto previo en el que se diseñen los modos o formas de actuación, la estructura jerárquica, el reparto de papeles y la continua o frecuente comunicación entre sus componentes. Atribuir todas estas condiciones a una persona que, excitada por sus inclinaciones sexuales, actuado en la intimidad de su domicilio, se incorpora a la red y facilita o participa en lo que, en términos internautas se denomina «Chat», me parece una desmesura difícilmente aceptable por el derecho penal (F.J.1).

2.2. AUTORIZACIÓN DEL JUEZ INSTRUCTOR

El apartado sexto del art. 282 bis de la LECrim dispone que "el Juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación (…)". La redacción dada a este precepto adolece de ciertas imprecisiones y omisiones, que debieran ser enmendadas a fin de establecer una clara delimitación competencial entre los diversos órganos intervinientes, enfatizando sobre cada uno de ellos su esfera de especialización en materia de investigación criminal.

Si bien el citado artículo atribuye, con absoluta claridad, al Juez la competencia para autorizar una infiltración informática, nada se dice en relación con el órgano encargado de tomar la iniciativa de recurrir a un agente encubierto. En buena lógica, la decisión relativa a la idoneidad de aplicar esta técnica de investigación solo puede recaer en manos de las Fuerzas y Cuerpos de Seguridad. Son los mandos encargados de cada operación quienes, sobre la base de sus conocimientos operativos y experiencia acumulada, están mejor cualificados para decidir sobre tan delicada cuestión. A idéntica conclusión podemos llegar acudiendo a una interpretación gramatical

de la norma, ya que el verbo elegido por el legislador en relación con la competencia del órgano judicial se concreta en "*autorizar*", no en decidir[7]. Así pues, las Fuerzas y Cuerpos de Seguridad, previa obtención de los datos suficientes y ponderación de las posibilidades de éxito -así como de los peligros inherentes a la infiltración- elaborarán un informe pormenorizado que será remitido al correspondiente órgano autorizante.

Habida cuenta de que la actuación de un agente de la Policía Judicial como infiltrado *on line*, supone una afectación de los derechos fundamentales de las personas inmersas en la investigación penal –particularmente el referido al secreto de las comunicaciones- se hace necesaria la intervención de un órgano judicial. En este sentido ha de interpretarse la apelación del apartado primero del art. 282 bis de la LECrim a la autorización de la operación policial encubierta por parte del Juez de instrucción. De la intervención del órgano instructor se deriva: bien el inicio de una instrucción judicial, bien la existencia de una instrucción previa. Sea de un modo u otro, la intervención obligada del Juez instructor implica que "el único marco procesal admisible para el desarrollo de una infiltración policial es el de una instrucción judicial" (Gascón, 2001).

El apartado 6 del art. 282 bis de la LECrim nada dice en relación con las características de la resolución, a través de la cual el órgano judicial autoriza la intervención del agente encubierto informático. A partir de una interpretación sistemática del artículo, se pueden considerar exigibles los requisitos establecidos por el apartado primero del citado precepto, esto es: que el auto judicial sea fundado y tenga presente la necesidad de la infiltración virtual, en relación a los fines de la investigación. En atención a la potencial minoración de derechos fundamentales derivada de la operación encubierta, debe rechazarse el recurso a fundamentaciones totalmente genéricas o estereotipadas. Debe recordarse que el propio Tribunal Constitucional (en adelante TC) desaconseja el uso de resoluciones judiciales de carácter impreso y estereotipado. Si bien el recurso a las mismas, no siempre provocará la existencia de una falta de motivación, ya que "peticiones idénticas pueden recibir respuestas idénticas, sin que la reiteración en la fundamentación suponga ausencia de esta, debiendo analizarse el caso concreto para determinar la suficiencia de la respuesta ofrecida" (STC, Sala Primera, 67/2000, de 13 marzo, RTC 2000\67, MP: Pablo Manuel Cachón Villar, FJ.3). A pesar de ello, el TC establece un deber de motivación reforzado para el caso de resoluciones judiciales que afecten a derechos fundamentales (STC, Sala Primera,116/1998, de 2 junio. RTC 1998\116, MP: Pedro Cruz Villalón, FJ. 4).

Al mismo tiempo, atendiendo a la injerencia en el derecho fundamental del secreto de las comunicaciones, derivada de la actividad del agente encubierto, serían aplicables –ante el silencio del art. 282 bis 6- los requisitos, de contenido mínimo, del auto judicial autorizante, que el artículo 588 bis c de la LECrim establece para el caso de interceptación de comunicaciones telemáticas. Por consiguiente, el auto judicial debe hacer referencia a:

- El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida. Para el caso particular objeto de análisis por este artículo, los hechos investigados se encontrarían tipificados en el artículo 189.1 b) del CP. En relación con la conceptualización de

7 En similares términos se pronuncian Expósito (2015) y Del Pozo (2006), en relación al agente encubierto físico, regulado en el artículo 282 bis 1 de la LECrim.

los indicios efectuada por la jurisprudencia, conviene recordar la definición de los mismos establecida por el TS, según el cual:

> Los indicios racionales de criminalidad, y a ello equivale la palabra «indicio» (…), son indicaciones o señas, o sea, datos externos que, apreciados judicialmente, conforme a normas de recta razón, permiten descubrir o atisbar, como dice la doctrina científica, sin la seguridad de la plenitud probatoria pero con la firmeza que proporciona una sospecha fundada, es decir, razonable, lógica, conforme a las reglas de la experiencia, la responsabilidad criminal de la persona en relación con el hecho posible objeto de investigación (…). No es ni puede ser, por consiguiente, un indicio la simple manifestación policial si no va acompañada de algún otro dato o de algunos que permitan al Juez valorar la racionalidad de su decisión en función del criterio de proporcionalidad. (ATS, Sala de lo Penal, de 18 junio 1992, RJ 1992\6102, MP: Enrique Ruiz Vadillo, FJ.2).

- La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido. Es posible que la identidad real de las personas, objeto de la investigación policial, no sea conocida en el momento de autorizar la infiltración. Debemos tener presente que la comunicación a través de Internet permite operar a través de un alias, por lo que el concepto identidad en este caso debe ser interpretado en sentido amplio, debiendo ser suficiente la indicación del *nick* con el que el investigado opera en la Red.

  La extensión de la medida de injerencia, especificando su alcance, así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a. Para el caso de infiltración virtual, la alusión a la extensión de la medida debe implicar una apelación, específica, a la posibilidad de que el agente de la Policía Judicial pueda enviar y recibir archivos ilícitos, así como analizar los resultados de los algoritmos para la identificación de los mismos.

  Los principios rectores mencionados por el artículo 588 bis a) de la LECrim son: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. Por lo tanto, el auto ha de dar cuenta de la aptitud de la medida para alcanzar el fin perseguido con ella, que no es otro que la determinación de los hechos que constituyen el objeto del proceso penal. Asimismo, deberá dejar constancia de que esta medida es imprescindible, no existiendo otra u otras menos gravosas, en clave de afectación de derechos fundamentales, con las que se puedan conseguir idénticos resultados. Por último, el auto judicial deberá dejar constancia de que la infiltración no supone un sacrificio desmedido de derechos en relación con la gravedad de los delitos perseguidos[8]. En relación con la gravedad del delito, en el supuesto de la distribución de pornografía infantil, hay que ir más allá del aspecto numérico o cuantitativo de la pena. En este caso, el mayor desvalor del injusto proviene de su nefasta incidencia en la infancia y de la peligrosidad ínsita en la propagación de este tipo de conductas.

- La unidad investigadora de Policía Judicial que se hará cargo de la infiltración.
- La duración de la medida.

8 En similar sentido vid. STC, Sala Primera, 207/1996, de 16 diciembre (RTC 1996\207, MP: Vicente Gimeno Sendra, FJ.4).

- La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados obtenidos.
- La finalidad perseguida con la medida.
- El sujeto obligado que llevará a cabo la infiltración: esto es identidad real y supuesta del infiltrado.

El respeto a estos requisitos, por parte del auto judicial, permitirá que los datos obtenidos gracias a la infiltración policial informática puedan convertirse en pruebas válidas, en el posterior juicio. La alusión a estas cuestiones dentro del auto, además de garantizar la protección de los derechos fundamentales de las personas investigadas, contribuye también a que el difícil y duro trabajo realizado por las Fuerzas y Cuerpos de Seguridad, durante la operación encubierta, pueda dar frutos y no se convierta en tiempo y esfuerzos desperdiciados, al verse invalidada legalmente la resolución judicial autorizante.

Sin desconocer la necesidad insoslayable de la autorización judicial de la infiltración policial, para el caso que nos ocupa, esta no debiera ser exigible *ab initio* en casos excepcionales, debiendo introducirse una reforma en este sentido dentro del texto del artículo 282 bis 6 de la LECrim. Se toma como referencia la posibilidad establecida por los artículos 579.3 y 588 ter d 3 de la LECrim. Según los citados preceptos, en casos de urgencia y para supuestos de averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas, se permite que la interceptación de las comunicaciones -bien postales y telegráficas, bien telefónicas y telemáticas- sea ordenada por el ministro del Interior -o, en su defecto, el secretario de Estado de Seguridad-, debiendo ser informado el juez competente, en el plazo máximo de 24 horas, a fin de que revoque o confirme la medida. Partiendo de dicha posibilidad, habilitada legalmente, se considera que debiera permitirse una solución similar para el caso de las operaciones encubiertas informáticas destinadas a luchar contra la pornografía infantil en Internet. Así pues, en casos excepcionales, en los que atendiendo a criterios operativos deba iniciarse de inmediato un contacto, en un canal cerrado *on line,* con las personas objeto de la investigación criminal, debiera facultarse al mando de la unidad orgánica de las Fuerzas y Cuerpos de Seguridad para ordenar dicha medida. De esta actuación tendría que darse cuenta inmediata al órgano judicial competente. Será la autoridad judicial, en última instancia, la encargada de avalar o rechazar el respeto de la medida en relación con los criterios de necesidad, proporcionalidad, idoneidad y excepcionalidad. No se trata en modo alguno de renunciar a las garantías del proceso penal. Tampoco es cuestión de retroceder en la indemnidad de los derechos fundamentales. Lo que se persigue con esta propuesta de reforma legal es dotar de mayor rapidez y flexibilidad a la fase de investigación criminal, adaptándola, en la medida de lo posible, al frenético ritmo marcado por la ciberdelincuencia.

2.3. LOS CONTACTOS PREVIOS

La infiltración con éxito, de un agente de la Policía judicial, no es una actividad susceptible de llevarse a cabo en un mínimo espacio de tiempo. Al contrario, es necesario un lapso temporal más o menos extenso en función de cada operación, en el cual el agente se pueda ir granjeando la confianza de los sujetos a investigar (García-Fustel, 2016). Por ello, la condición formal de agente encubierto, atribuida mediante auto judicial, es posterior al inicio de la actividad real de infiltración.

La cuestión relativa a la validez de estas actuaciones del agente, previas a la autorización judicial, ha sido analizada por la jurisprudencia. Se admite el pleno encaje legal de la actividad del agente, previa al *placet* judicial, tendente a generar unos imprescindibles vínculos ficticios de camaradería con los investigados. Particularmente ilustrativa sobre esta materia resulta la STS, Sala de lo Penal, Sección 1ª, 575/2013, de 28 de junio (RJ 2013\8067, MP: Manuel Marchena Gómez), en la cual el Alto Tribunal afirma, en relación a la infiltración en un grupo criminal, que:

es contrario a las elementales máximas de experiencia concebir la infiltración en un grupo criminal como la respuesta a una invitación formal a un tercero que, de modo inesperado, curiosea entre los preparativos de una operación delictiva. La autorización judicial, por sí sola, no abre ninguna puerta al entramado delictivo que quiere ser objeto de investigación. Antes al contrario, la cerraría de forma irreversible. De ahí que esta resolución tiene que producirse en el momento adecuado que, como es lógico, no tiene por qué ser ajeno a una relación previa que contribuya a asentar los lazos de confianza. (FJ. 2)

En idéntica línea la STS, Sala de lo Penal, Sección 1ª, 277/2016, de 6 abril, (RJ 2016\1325, MP: Antonio del Moral García), indica que:

cuestionar la existencia de investigaciones previas a la entrada en acción del agente encubierto como tal, y, al mismo tiempo, pedir que su habilitación cuente con apoyo en elementos de juicio dotados de suficiente base empírica para dar racionalidad a la medida, tiene algo de contradictorio. En el caso, no cabe duda, los propios datos aportados ahora por el recurrente y que constan en las actuaciones, permiten advertir que quien luego se convertiría en agente encubierto, venía actuando durante algunos meses, antes de recibir esta investidura judicial conforme a la ley; es decir, ejerciendo, pura y simplemente, un cometido propio de policía, (…). Y lo cierto es que lo que consta al respecto no sugiere la existencia de ninguna incorrección. Y, no solo, sino que, a tenor de todo lo que ahora se sabe, cabe hablar más bien de un comportamiento regular, pues desembocó en la solicitud de esa especial cobertura judicial, justo cuando el desarrollo de los acontecimientos iba a exigir del agente una mayor y más delicada implicación en ellos... (FJ. 1)

Ambas resoluciones del TS, siguiendo la estela trazada por otras sentencias anteriores, reconocen la validez probatoria de la información obtenida por el miembro de las Fuerzas y Cuerpos de Seguridad antes de conseguir judicialmente su condición de agente encubierto. Los datos obtenidos, durante esos contactos previos, serán traspasados al plenario, a través de la declaración del agente en calidad de testigo.

2.4. LA POLICÍA JUDICIAL

Conforme el tenor del artículo 282 bis 6 de la LECrim, la autorización judicial habilita exclusivamente a los agentes de la Policía Judicial a actuar bajo una identidad supuesta. Dentro de la pirámide jurídica kelseniana española, la primera referencia legal a la Policía Judicial la encontramos en el artículo 126 Constitución Española (BOE nº 311, de 29 de diciembre de 1978) (en adelante CE), en el que se establece que "la policía judicial depende de los Jueces, de los Tribunales y del Ministerio Fiscal en sus funciones de averiguación del delito y descubrimiento y aseguramiento del delincuente, en los términos que la ley establezca". Partiendo de este postulado constitucional, a nivel doctrinal, la Policía Judicial se configura, según Queralt (1999), como:

una función específica dentro de las funciones de la Policía General, basada en los criterios de la Policía científica, destinada a la investigación de los hechos punibles, la persecución y aseguramiento de los delincuentes, poniendo a disposición de la autoridad judicial y eventualmente, del Ministerio Fiscal, los resultados de su averiguación (p.13).

Sus funciones sirven al proceso penal, ya sea actuando con carácter previo a la intervención judicial, ya sea actuando en diligencias practicadas durante el propio proceso penal (Moreno, 1989).

El problema en relación a la Policía Judicial surge, no a nivel conceptual, sino en relación con la delimitación de sus integrantes y del modelo instaurado. Las previsiones constitucionales del artículo 126 de la CE no han sido desarrolladas mediante una legislación integral sobre la Policía Judicial, encontrándose su regulación dispersa en múltiples normas, de variado objeto y rango normativo. En este artículo se hará, exclusivamente, referencia a aquellas normas que interesan a los efectos de determinar qué funcionarios públicos pueden actuar como agente encubierto informático, en la persecución de la ciberdelincuencia relacionada con la pornografía infantil. En este orden de cosas, nuestra vetusta ley procesal penal, en su artículo 283, ofrece un catálogo de figuras componentes de la Policía Judicial. Dicho precepto data del año 1967[9], por lo que algunas de las figuras enunciadas se encuentran desfasadas o desaparecidas. Se expresa así un modelo de Policía Judicial denominado genérico o de primer grado, vinculado a la obligación genérica de auxiliar a la Justicia, plasmada en el artículo 118 de la CE.

Una delimitación más concreta, acorde con la realidad actual y fiel a los principios de unidad de dirección y especialización, la encontramos en el artículo 7 del Real Decreto 769/1987, de 19 de junio, sobre regulación de la Policía Judicial (BOE nº 150, de 24 de junio de 1987). Se plasma, en este caso, un modelo de Policía Judicial específica o en sentido estricto. Dicho precepto establece que "constituyen la Policía Judicial en sentido estricto las Unidades Orgánicas previstas en el artículo 30.1 de la Ley Orgánica de Fuerzas y Cuerpos de Seguridad integradas por miembros del Cuerpo Nacional de Policía y de la Guardia Civil". En este punto cabe recordar que el artículo 29.2 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad (BOE nº 63, de 14 de marzo de 1986) (en adelante LOFCS), atribuye el carácter de colaborador de la Policía Judicial al personal de Policía de las Comunidades Autónomas y de las Corporaciones Locales.

Coexistiendo legalmente, de modo pacífico, con la anterior previsión de la LOFCS, hay que señalar que, los Estatutos de Autonomía de País Vasco, Cataluña y Navarra –así como sus respectivas normas reguladoras de las correspondientes policías autonómicas- han previsto la creación de Unidades Orgánicas de la Ertzaintza, de los Mossos d´Esquadra y de la Policía Foral de Navarra, con competencias en materia de Policía Judicial[10]. Por lo tanto, respetando siempre los criterios de territorialidad y de

9 Artículo 283 de la LECrim redactado por Ley 3/1967, de 8 de abril, sobre modificación de determinados artículos del Código Penal y de Ley de Enjuiciamiento Criminal (BOE nº 86, de 11 abril de 1967).

10 Para el caso del País Vasco vid: Artículo 17.3 de la Ley Orgánica 3/1979, de 18 de diciembre, de Estatuto de Autonomía para el País Vasco (BOE nº 306, de 22 de diciembre de 1979). Artículos 112 a 115 de la Ley 4/1992, de 17 de julio, de Policía del País Vasco (BOPV nº155, de 11 de agosto de 1992; BOE nº 39, de 15 de febrero de 2012). Para el caso de Cataluña vid: Artículo 164.5 c) de la Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de Autonomía de Cataluña (BOE nº 172, de 20 de Julio de 2006). Artículos 13 a 15 de la Ley 10/1994, de 11 de julio, de la Policía de la Generalidad de Cataluña "Mossos d'Esquadra" (DOGC nº. 1923, de 20 de Julio de 1994; BOE nº. 192, de 12 de agosto de 1994). Para el caso de Navarra vid: Artículo 51 de la Ley Orgánica 13/1982, de 10 de agosto, de reintegración y amejoramiento del Régimen Foral de Navarra (BOE nº. 204, de 16 de agosto de 1982). Artículo 13 de la Ley Foral 8/2007, de 23 de marzo, de las Policías de Navarra (BON nº. 40, de 2 de abril de 2007; BOE nº. 100, de 26 de abril de 2007)

especialización delictual –establecidos por el artículo 30.1 de la LOFCS- los miembros de la Policía Judicial que actuarán como agentes encubiertos virtuales podrán provenir del Cuerpo Nacional de Policía, de la Guardia Civil, de los Mossos d´Esquadra, de la Ertzaintza y de la Policía Foral de Navarra.

En relación con las policías dependientes de las Corporaciones Locales, su intervención, en cuanto agentes encubiertos, queda absolutamente descartada legalmente. El *Convenio Marco de Colaboración, Cooperación y Coordinación entre el Ministerio del Interior y la Federación Española de Municipios y Provincias* -suscrito el 20 de febrero de 2007- permite que la Policía Local de aquellas Corporaciones Locales que se adhieran al mismo ejecuten funciones de policía judicial, tanto en lo que se refiere a la recepción de denuncias, como a la investigación de los hechos. No obstante, la posibilidad de intervención de la Policía Local queda circunscrita a una lista cerrada de infracciones penales, entre las que no se encuentran los ilícitos del artículo 189 del CP. Además, la infiltración policial requiere un alto grado de capacitación y especialización de los agentes que han de llevarla a cabo. Este elevado nivel de conocimientos y de experiencia operativa solo concurre, por el momento, en el Cuerpo Nacional de Policía, la Guardia Civil y determinadas policías autonómicas.

2.5. VOLUNTARIEDAD DEL AGENTE

El artículo 282 bis 6 LECRIM nada dice en relación a la voluntariedad de la función de agente encubierto informático. En cambio, para el caso de su homólogo, el agente encubierto físico, el apartado 2 del mentado precepto de la LECrim afirma, de modo taxativo, que ningún funcionario de la Policía Judicial podrá ser obligado a actuar como agente encubierto. Acudiendo a una interpretación sistemática, se concluye que el requisito de voluntariedad del agente también es predicable respecto del infiltrado informático.

La necesidad de que el agente consienta libremente su participación como agente infiltrado, deriva de la peligrosidad ínsita a este tipo de operaciones. Si bien es cierto que la infiltración física conlleva un mayor grado de exposición del agente a diferentes riesgos, no resulta menos cierto que la infiltración virtual no resulta inocua para el policía que la lleva a cabo. Pensemos, por ejemplo, en las nocivas consecuencias, de tipo psicológico, que puede acarrear el hecho de mantener conversaciones habituales con pedófilos, haciéndose pasar por uno de ellos; así como el visionado constante del material que intercambian estos delincuentes. A mayor abundamiento, hay que señalar que los modos de contacto a través de Internet no se circunscriben al simple intercambio de mensajes escritos. Existen programas informáticos que permiten la realización de videollamadas (Skype, Facebook, etc). En tales supuestos, el agente infiltrado informático podría llegar a mostrar su aspecto físico, siendo plenamente reconocible por los delincuentes. Todo ello determina que deba ser el propio agente, quien de modo libre, acepte ejecutar este tipo de operaciones encubiertas; no pudiendo ser compelido a ello, ni por la autoridad judicial ni por sus superiores jerárquicos.

2.6. ÁMBITO DE ACTUACIÓN: LOS CANALES CERRADOS DE COMUNICACIÓN

El artículo 282 bis 6 de la LECrim circunscribe el ámbito de actuación de la infiltración del agente virtual a “las comunicaciones mantenidas en canales cerrados”.

Otra de las deficiencias omisivas del precepto analizado –amén de las ya citadas- se concreta en la ausencia de definición legal del vago concepto "*canales cerrados*", que en este caso actúa como punto fronterizo del campo de actuación de la infiltración policial. Las llamadas comunicaciones en canal cerrado, "se caracterizan por la expresa voluntad del comunicante de excluir a terceros del proceso de comunicación" (STS, Sala de lo Penal, Sección 1ª, 249/2008, de 20 de mayo, RJ 2008\4387, MP: Manuel Marchena Gómez, FJ. 4). En atención a lo cual, la cualidad de cerrado de un canal de comunicación ha de derivarse de la existencia de un requisito previo de aceptación, por parte del interlocutor, de cada una de las personas que van a formar parte de su grupo de contactos de confianza. De este modo, el interlocutor elimina el carácter de público de determinados contenidos, por él seleccionados, que únicamente son accesibles a determinadas personas seleccionadas (Valverde, 2015).

Si los canales de comunicación no son cerrados, no será necesario el recurso a la figura legal del agente encubierto. Los Cuerpos Policiales podrán rastrear los contenidos de la Red, que revistan carácter público, sin ninguna garantía adicional más allá de la correspondiente habilitación legal. Dicha habilitación legislativa ha de considerarse comprendida, dentro de las facultades atribuidas a las Fuerzas y Cuerpos de Seguridad, por el artículo 11 de la LOFCS y el artículo 282 de la LECrim (Cabezudo, 2016). A este respecto conviene recordar lo dispuesto en la STS, Sala de lo Penal, Sección 1ª, 236/2008, de 9 de mayo (RJ 2008\4648, MP: José Ramón Soriano Soriano). Esta resolución entraba a valorar la legalidad de unos rastreos en Internet, realizados por el Equipo de delitos telemáticos de la Guardia Civil, al objeto de desenmascarar la identidad críptica de los IPS (Internet protocols) que habían accedido a unos *hash* que contenían pornografía infantil. El Alto Tribunal concluyó que:

> *el acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma. La huella de la entrada - como puntualiza con razón el Mº Fiscal- queda registrada siempre y ello lo sabe el usuario (FJ.2).*

Siguiendo la misma línea, otra resolución del TS, en este caso la STS Sala de lo Penal, Sección 1º, 767/2007, de 3 de octubre (RJ 2007\7297, MP: José Ramón Soriano Soriano) admitió la plena legalidad de los contactos mantenidos por un agente de la Guardia Civil -bajo un *nick* falso y sin contar con la condición de agente encubierto-, en un chat ubicado en un canal IRC, con la finalidad de localizar a un pedófilo que suministraba pornografía infantil a través de la Red (F.J 4º).

Las Fuerzas y Cuerpos de Seguridad, por lo tanto, pueden realizar actividades de ciberpatrullaje en canales abiertos de comunicación (tales como foros abiertos de internet, redes sociales y redes *peer to peer*), interactuando con otras personas bajo *nicks* ficticios, sin que ello tenga que estar autorizado judicialmente. Esta actividad policial se enmarca dentro de las funciones legales de vigilancia, prevención y evitación de delitos. Téngase presente, a este respecto, que los actuales usos sociales permiten que las personas que se relacionan en Internet con otros usuarios, empleando para ello *nicks*, admiten y consienten que la persona con la que se comunican no posee realmente esa identidad (Zaragoza, 2017).

2.7. FACULTADES DEL AGENTE ENCUBIERTO: EL PROBLEMA DEL INTERCAMBIO DE ARCHIVOS

La LECrim faculta al agente encubierto informático para realizar tres tipos de actuaciones: a) operar en el tráfico social, de los canales de comunicación cerrados, bajo una identidad ficticia, que esconda su condición de miembro de las Fuerzas y Cuerpos de Seguridad; b) intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido; c) analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.

De las tres facultades atribuidas al agente encubierto informático, en relación con el delito de distribución de pornografía infantil, la más polémica resulta la posibilidad de intercambio o envío de material ilícito por parte de un miembro de la Policía Judicial. La generación de un vínculo de confianza, entre el pedófilo y el agente encubierto, requiere –irremediablemente- que este efectúe una aportación de material ilícito, con la finalidad de hacer creer al delincuente que se comunica con una persona que comparte los mismos abominables gustos que él. Esta actuación del agente encubierto hace surgir dos cuestiones controvertidas.

En primer lugar, hay que determinar el origen del material pedófilo destinado a ser remitido al delincuente por parte de la Policía Judicial. Respecto a este interrogante se han apuntado, a nivel doctrinal, dos soluciones posibles: el recurso a material incautado en operaciones anteriores; o la elaboración de material pornográfico *ad hoc*, protagonizado por actores mayores de edad, pero cuyo físico pueda conducir a error sobre su verdadera edad (Bueno de Mata, 2012).

Respecto de la última solución apuntada, estimo que su aplicación puede resultar contraproducente, a efectos de obtener una condena penal del delincuente. Si el material aportado por la Policía Judicial está protagonizado por actores adultos, la defensa del delincuente puede argumentar que su cliente era plenamente conocedor de la mayoría de edad de dichos actores, eliminando así el reproche penal de la actuación de su defendido. Otra posible estrategia letrada puede consistir en generar dudas sobre la apariencia de minoría de edad de los actores, en tal caso -por el juego del principio *in dubio pro reo*- podría llegarse también a una resolución absolutoria del procesado. Además, dependiendo de las inclinaciones pedófilas de los criminales, puede ser necesario que los menores sean de corta edad, por lo que sería imposible recurrir a actores adultos que se hagan pasar por niños o niñas.

El recurso a archivos pedófilos, procedentes de operaciones anteriores, resultará más eficaz para la investigación. Ahora bien, el uso de este material debe realizarse atendiendo a criterios de excepcionalidad, necesidad y proporcionalidad. De tal forma que el fin perseguido, la importancia del delito y la envergadura de la operación policial deben ser puestos en relación con las características del material que se vaya a poner en circulación. A este respecto, habrá que valorar, por ejemplo, el carácter particularmente degradante o la corta edad de los menores que aparezcan en los archivos (Rodríguez, 2015).

Ha de descartarse, de plano, que el intercambio o el envío de archivos pedófilos, realizado por el agente infiltrado, ultrapase la frontera del delito provocado, proscrita por el artículo 282 bis 5 de la LECRIM. En palabras del TS:

no existe delito provocado, como dice la Sentencia 1114/2002, de 12 de junio, cuando los agentes de la autoridad sospechan o conocen la existencia de una actividad delictiva y se infiltran entre quienes

la llevan a cabo, en busca de información o pruebas que permitan impedir o sancionar el delito. En estas ocasiones, la decisión de delinquir ya ha surgido firmemente en el sujeto con independencia del agente provocador, que, camuflado bajo una personalidad supuesta, se limita a comprobar la actuación del delincuente e incluso a realizar algunas actividades de colaboración con el mismo, en la actualidad reguladas, desde la entrada en vigor de la Ley Orgánica 5/1999, de 13 de enero, en el artículo 282 bis de la Ley de Enjuiciamiento Criminal, que se refiere concretamente a adquirir y transportar los objetos, instrumentos o efectos del delito. La intervención policial puede producirse en cualquier fase del "iter criminis", en el momento en que el delito ya se ha cometido o se está cometiendo, especialmente en delitos de tracto sucesivo como los de tráfico de drogas, y aun en sus fases iniciales de elaboración o preparación, siendo lícita mientras permita la evolución libre de la voluntad del sujeto y no suponga una inducción a cometer el delito que de alguna forma la condicione. En estos casos, la actuación policial no supone una auténtica provocación, pues la decisión del sujeto activo es siempre libre y anterior a la intervención puntual del agente encubierto, aunque este, siempre por iniciativa del autor de la infracción criminal, llegue a ejecutar labores de adquisición o transporte de los efectos del delito (art. 282 bis de la LECrim), u otras tareas de auxilio o colaboración similares, simulando así una disposición a delinquir que permite una más efectiva intervención policial. (STS, Sala de lo Penal, Sección 1ª, 104/2011, de 1 de marzo, RJ 2011\2499, MP: Juan Ramón Berdugo y Gómez de la Torre, FJ 2).

Esta facultad del agente encubierto *on line,* de enviar o intercambiar material ilícito, es en esencia una figura híbrida. Está a medio camino entre la facultad del agente encubierto físico, relativa a "adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos", y la técnica de investigación denominada entrega vigilada, del artículo 263 bis de la LECrim (Cabezudo, 2016). Habida cuenta de la similitud existente con la entrega vigilada, la cual puede ser autorizada por los jefes de las Unidades Orgánicas de la Policía Judicial -centrales o de ámbito provincial- o sus mandos superiores, se entiende que podría haberse habilitado idéntica posibilidad de autorización para los mandos de la Policía Judicial, en el caso del intercambio o envío de material pedófilo, siempre y cuando se diese cuenta de inmediato al juez instructor.

3. CONCLUSIONES

El uso de las nuevas tecnologías es una característica central de esta nueva etapa histórica que conocemos como *globalización*. Más allá de sus cualidades positivas, Internet se ha revelado como el escenario óptimo para la distribución de material pornográfico, en el que los menores son víctimas de abusos y agresiones.

Los códigos de sociabilidad, empleados en este medio, permiten que los internautas puedan interactuar con un simple alias, sin necesidad de dar a conocer su verdadera identidad. Este anonimato, consentido y aceptado por los usuarios, facilita el desarrollo de actividades criminales, ya que los delincuentes encuentran una primera capa de protección en el empleo de un alter-ego virtual. A ello debemos sumar el desvanecimiento de las barreras físicas y temporales y el control mínimo de la información, que caracteriza el tráfico en Internet. Un documento puede ser enviado de un continente a otro en cuestión de segundos, sin que ninguna autoridad estatal lo controle. La aparición constante de nuevos programas informáticos permite la creación de archivos cada vez más complejos, dotados de unas mayores medidas de restricción de acceso.

Esta nueva realidad delictiva, que emplea Internet como medio de difusión, desborda, en gran medida, aquella para la que fue creada la mayoría del Derecho penal aún vigente. Es imprescindible, en consecuencia, contemporizar nuestra legislación punitiva al incontenible ritmo marcado por la ciberdelincuencia. La descripción de las

conductas perseguidas penalmente, así como los medios de investigación empleados, deben resultar efectivos en un contexto que experimenta constantes cambios. Al mismo tiempo, debemos salvaguardar la indemnidad de principios penales básicos, como el de legalidad o el de seguridad jurídica, con los que se impiden afectaciones desmedidas de derechos fundamentales, impropias de cualquier Estado de Derecho.

En relación con la distribución de material pedófilo a través de Internet, la inclusión en el artículo 189.1 b) del CP de un concepto formal de pornografía infantil, imposibilita la persecución penal de la distribución de soportes en los que se incluyan imágenes de menores que, pese a estar desprovistas en apariencia de contenido sexual explícito, son empleadas y distribuidas por los pedófilos para un uso libidinoso. De igual modo, la exigencia legal relativa a que el archivo pornográfico sea visual, impide la persecución penal de escritos o audios en los que se recojan las agresiones sexuales de las que son objeto los niños y las niñas objeto de tan execrable material. La atribución del carácter pedófilo, efectuado por parte del aplicador del Derecho –no por parte del legislador-, permitiría una mayor adaptación de la respuesta penal a las mutaciones incesantes de esta forma de criminalidad *on line*.

La inclusión de la figura del agente encubierto informático, en la legislación procesal penal española, ha sido un paso importante -y necesario- para adaptar nuestros medios de investigación criminal a las peculiares características de la ciberdelincuencia. No obstante, el diseño legal realizado lo convierte en una figura que presenta múltiples interrogantes y un elevado grado de rigidez procedimental. El apartado sexto del artículo 282 bis de la LECrim, precepto regulador de esta técnica de investigación policial, guarda silencio en relación al contenido mínimo del auto judicial autorizante.

Esta laguna jurídica no es admisible respecto de una resolución que provoca una injerencia en el secreto de las comunicaciones. Para preservar la indemnidad de los derechos fundamentales afectados por la actuación del agente encubierto informático, así como para salvaguardar el fruto del trabajo realizado por la Policía Judicial durante la infiltración, debiera haberse incluido en la LECrim una referencia, explícita, a las cuestiones mínimas que deben quedar reflejadas en el auto autorizante -tal y como ocurre en el caso de la interceptación de comunicaciones, regulada en el artículo 588 bis c del citado texto procesal-. En este mismo sentido, otra de las deficiencias legales omisivas se encuentra en la delimitación del campo de actuación del agente infiltrado virtual. El empleo, en el artículo 282 bis 6 de la LECrim, de la expresión canales cerrados para referirse al campo de las comunicaciones en las que pueden infiltrarse las Fuerzas y Cuerpos de Seguridad, no va acompañado de una definición de tan vago concepto. Se genera, de este modo, una situación de inseguridad jurídica que dificulta el resultado de la labor policial. Por último, en lo que a silencios legislativos se refiere, hay que reseñar que la atribución legal al agente encubierto informático de la posibilidad de intercambiar o enviar archivos ilícitos debiera ir acompañada de una mención expresa a la posibilidad de emplear material incautado en operaciones anteriores.

La atribución de más competencias a las Fuerzas y Cuerpos de Seguridad, dentro del procedimiento establecido por la LECrim, agilizaría la aplicación de este medio de investigación, adaptándose mejor a la acelerada velocidad del universo virtual. En este sentido, el control judicial de la infiltración no tendría que ser exigible ab initio para todos los casos, pudiendo ser desplazado a un momento posterior del procedimiento. En aquellos casos en los que, razones operativas de urgencia, aconsejen un

inicio inmediato de la actuación del agente encubierto, dicha intervención podría ser autorizada por los mandos de las unidades orgánicas de las Fuerzas y Cuerpos de Seguridad. De modo similar a lo dispuesto en relación con la posibilidad, ya establecida en la propia LECrim, respecto de la interceptación de comunicaciones para la averiguación de delitos relacionados con la actividad terrorista. A idéntica conclusión se puede llegar en relación con la autorización judicial del intercambio de material pedófilo. En este caso, los mandos de la Policía Judicial podrían autorizar inicialmente dicho intercambio –al igual que sucede en las denominadas entregas vigiladas del artículo 263 bis de la LECrim- dando cuenta posteriormente al órgano judicial instructor.

La incorporación de la figura del agente encubierto informático, dentro del ordenamiento procesal penal español, resulta positiva en cuanto adaptación de los tradicionales mecanismos de investigación criminal a las nuevas realidades condicionadas por la comunicación a través de la Red. Sin embargo, ese juicio inicial favorable queda desvirtuado por la implementación de un diseño legislativo marcado por un excesivo rigorismo procedimental y por el recurso a conceptos jurídicos indeterminados.

BIBLIOGRAFÍA

Bueno de Mata, F. (2012). El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia. En Pérez-Cruz A.J (coord.), *Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal (Internacional) A Coruña, 2 y 3 de junio de 2011* (pp. 295-306). A Coruña: Universidade da Coruña, 2012.

Cabezudo, N. (2016). Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. *Boletín del Ministerio de Justicia*, 2186, 7-60.

Cruz, J.A. (2006). *Derecho penal y nuevas tecnologías. Aspectos sustantivos*. Madrid: Grupo Difusión.

Del Pozo, M. (2006). El agente encubierto como medio de investigación de la delincuencia organizada en la Ley de Enjuiciamiento Criminal española. *Criterio Jurídico*, 6, 267-310.

Expósito, L. (2015). El agente encubierto, *Revista de Derecho UNED* , 17, 251-286.

García-Fustel, J. (2016). Figuras de agente encubierto y confidente visión de la Guardia Civil. Ponencia presentada en las jornadas *La prueba obtenida a través de la infiltración y la delación. El Agente Encubierto y el confidente*, organizadas por el del Ministerio Fiscal y celebradas el 2 de junio de 2016. Recuperado de: www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/comunicaciónGarcía-FustelGonzález, Jesús.pdf?idFile=f7cb2112-9d7c-4a2c-9d17-51efae9a0197.

García, C. (2004). Acerca del delito de pornografía infantil. En Octavio, E. (Coord), *Estudios penales en recuerdo del profesor Ruiz Antón* (pp. 411-430). Valencia: Tirant lo Blanch.

Gascón, F. (2001). *Infiltración policial y «agente encubierto.* Granada: Comares.

Guisado, A. (2007). El consumo de pornografía infantil en Internet. El lado oscuro de

la Red. *Revista de Contratación Electrónica*, 81, 3-45 .

Jiménez, J. (2012). Tráfico de pornografía infantil: dinámica, roles y prevención. *Gaceta Internacional de Ciencias Forenses*, 5, 33-41.

Jenkins, P. (2001). *Beyond Tolerance: Child Pornography on the Internet*. New York: University Press.

Lemineur, M.L. (2006). *El combate contra la pornografía infantil en Internet. El caso de Costa Rica*. San José: ADC Asesoría Creativa S.A.

Moreno, V. (1989). Dependencia orgánica y funcional de la Policía Judicial. *Revista del Poder Judicial*, nº. Especial VIII, 139-154.

Negredo, L. y Herrero, P. (2016). Pornografía infantil en Internet. *Papeles del Psicólogo,* 37(3), 217-223.

Querált, J. (1999). *Introducción a la Policía Judicial*. Barcelona: Bosch.

Rodríguez, M.V. (2015). "La infiltración policial: en el límite del Estado de Derecho. El inminente agente encubierto informático" Recuperado de: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10222-la-infiltracion-policial:-en-el-limite-del-estado-de-derecho-el-inminente-agente-encubierto-informatico/

Roxin, C. (2013). El concepto de bien jurídico como instrumento de critica legislativa sometido a examen. *Revista electrónica de Ciencia Penal y Criminología*, 15.

Ruiloba, J.C. (2006). La actuación policial frente a los déficits de seguridad de Internet. *Revista de Internet, Derecho y Política*, 2.

Salom, J. (2007). Pornografía infantil en internet. *Cuadernos de la Guardia Civil. Revista de Seguridad Pública*, XXXVI, 17-24.

Salom, J. (2009). Delito Informático y su Investigación.P ponencia presentada en el *XX Seminario Duque de Ahumada: seguridad y nuevas tecnologias*. Recuperado de: http://portal.uned.es/pls/portal/docs/PAGE/UNED_MAIN/LAUNIVERSIDAD/UBICACIONES/06/DUQUE_AHUMADA/PONENCIAS%20XX%20SEMINARIO%20DUQUE%20DE%20AHUMADA/4.PDF.

Taylor, M. y Quayle, E. (2003). *Child Pornography. An Internet Crime*. New York: Brunner-Routledge.

Valverde, R. (2015). Cuestiones procesales relativas a la investigación de los delitos en Red. *Ponencias de formación continuada del Ministerio Fiscal*. Recuperado de: www.fiscal.es/fiscal/publico/ciudadano/documentos/ponencias_formacion_continuada/

Zaragoza, F.I. (2017). El agente encubierto «online»: la última frontera de la investigación penal. *Revista Aranzadi Doctrinal*, 1/2017.

Fecha de recepción: 08/09/2017. Fecha de aceptación: 18/12/2017