MODO DE ACTUACIÓN DEL AGENTE ENCUBIERTO VIRTUAL

Mode of operation of the virtual undercover agent

Por Arantza León Camino

Abogada del Ilustre Colegio de la Abogacía de Madrid (ICAM) y Doctora en Derecho por la Universidad Carlos III de Madrid (UC3M)

arantzaleoncamino@hotmail.com

Artículo recibido: 15/11/23 | Artículo aceptado: 06/01/24

RESUMEN

La figura del agente encubierto virtual surge de la clara necesidad de terminar con los delitos cometidos a través de la red, que van cogiendo fuerza por el avance de las nuevas tecnologías y los sistemas informáticos. En internet, saltarse los controles policiales y, en general, saltarse la ley y las normas, es mucho más fácil que en la vida real. Es este el principal motivo por el que era necesaria una reforma y era necesario que el Estado controlara de una forma distinta la delincuencia informática.

La reforma de la Ley de Enjuiciamiento Criminal del 2015 era necesaria para intentar acabar con delitos que lesionan gravemente los bienes jurídicos protegidos por el derecho penal y que son repulsivos para la gran mayoría de la sociedad, como son, el de pornografía infantil o delitos relacionados con el ciberterrorismo como el de captación de miembros para bandas terroristas.

Para poder comprender cómo puede actuar un policía encubierto de forma virtual, nos debemos situar en un escenario en el que ha sido admitida la infiltración policial por su correspondiente autorización judicial, y el policía en cuestión se infiltra virtualmente. En este contexto, el agente encubierto virtual está facultado para realizar ciertas actividades que están permitidas por parte del Estado, y lo están a pesar de que pueden resultar limitativas de derechos fundamentales. La justificación de que el Estado permita al agente encubierto virtual desarrollar determinadas actividades es la de erradicar los delitos que se están ejecutando a través de la red.

ABSTRACT

The figure of the virtual undercover agent arises from the clear need to put an end to crimes committed through the internet, which are gaining strength due to the advance of new technologies and computer systems. On the internet, bypassing police controls and, in general, breaking the law and the rules, is much

easier than in real life. This is the main reason why reform was necessary and why the state needed to control cybercrime in a different way.

The reform of the Criminal Procedure Act of 2015 was necessary to try to put an end to crimes that seriously harm the legal assets protected by criminal law and that are repulsive to the vast majority of society, such as child pornography or crimes related to cyberterrorism such as the recruitment of members for terrorist gangs.

In order to understand how a virtual undercover police officer can act, we must situate ourselves in a scenario in which police infiltration has been admitted by corresponding judicial authorization, and the police officer in question infiltrates virtually. In this context, the virtual undercover agent is empowered to carry out certain activities that are permitted by the state, even though they may be restrictive of fundamental rights. The justification for the state allowing the virtual undercover agent to carry out certain activities is to eradicate crimes that are being executed through the network.

PALABRAS CLAVE

Agente encubierto virtual, Canal comunicación cerrado, Intercambio archivos ilícitos, Análisis algoritmos, Ley Enjuiciamiento Criminal.

KEYWORDS

Virtual undercover agent, Closed communication channel, Illegal file sharing, Algorithm analysis, Criminal Procedure Law.

1. Modo de actuación del agente encubierto virtual en la Ley Orgánica 13/2015

Para comprender correctamente la actuación del agente encubierto virtual o informático (en adelante, AEV), es preciso situarnos en un contexto en el que se ha otorgado la autorización judicial inicial correspondiente, la que le autoriza a actuar bajo identidad supuesta. Pero para desarrollar determinadas actuaciones, debe existir una autorización judicial específica, sea en la misma resolución judicial inicial, sea en otra distinta, en todo caso, con motivación separada y suficiente.

La exposición de motivos de la Ley Orgánica 13/2015[1], en concreto en su Capítulo IV, establece las actividades que puede desarrollar el AEV:

"de una parte se prevé la posibilidad de que los agentes encubiertos puedan obtener imágenes y grabar conversaciones, siempre que recaben específicamente una autorización judicial para ello; (…) y que, a su vez, requerirá una autorización especial (sea en la misma resolución judicial, con motivación separada y suficiente, sea en otra distinta) para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación".

Debido a esta Ley Orgánica, por la que se actualiza y reforma la Ley de Enjuiciamiento Criminal (en adelante, LECrim), el Estado faculta al AEV, según los apartados 6 y 7 del art. 282 bis de la LECrim, con autorización específica, a:

"intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos."

El Juez también podrá autorizar:

"la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio".

Por lo expuesto, podemos afirmar que el AEV podrá: 1. Enviar archivos que por su contenido puede ser considerado ilícito; 2. Analizar algoritmos que se han utilizado para la identificación de los archivos; y 3. Realizar imágenes o grabar determinadas conversaciones privadas que se han cometido con el sujeto investigado.

Para desarrollar todas estas actuaciones, la autorización judicial habilitante deberá reunir ciertos requisitos esenciales de legitimidad constitucional[2].

[1] España. 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. Boletín Oficial del Estado núm. 239, 6 de octubre de 2015.

[2] España. Tribunal Supremo. Sentencia núm. 65/2019, de 7 de febrero (TOL7.059.509).

2. Actuación a través de canales de comunicación cerrados

La ya mencionada Ley Orgánica 13/2015, de modificación de la LECrim, en su exposición de motivos, capítulo IV, "*regula la figura del agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación (puesto que, en los canales abiertos, por su propia naturaleza, no es necesaria)*".

El ámbito normal de actuación del AEV será el de mantener conversaciones, e interactuar con el investigado en la red. Destacamos la SAN, Secc. 3ª, núm. 33/2018, de 25 de septiembre, en la que podemos observar cómo se autoriza una infiltración en un perfil de Facebook, y tiempo después, se le habilita para crear otros perfiles en otras redes sociales como Twitter, Badoo, Telegram o Whatsapp[3].

Bajo una identidad supuesta, y con el objetivo de esclarecer determinados delitos, el AEV podrá actuar en comunicaciones mantenidas en canales de comunicación cerrados[4]. Para actuar en este tipo de canales necesitará la correspondiente autorización judicial inicial, lo que no es necesario cuando actúa en canales de comunicación abiertos, en los que su actuación no atenta a derechos fundamentales con protección reforzada. A la autorización judicial que nos referimos es a la que faculta al AEV para actuar bajo identidad supuesta. Para realizar otro tipo de actuaciones más específicas se requiere una autorización expresa.

[3] España Sentencia Audiencia Nacional, Secc. 3ª, núm. 33/2018, de 25 de septiembre (TOL6.814.961).

[4] España. Tribunal Constitucional. Sentencia núm. 170/2013, de 7 de octubre (TOL3.992.610), que expone que ha de entenderse por canal de comunicación cerrado "*aquel en el que existe una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas*", es decir, aquellos casos "*en los que la comunicación requiera una previa invitación para poder incorporarse al canal de comunicaciones*". También destacamos la STS núm. 357/2021, de 29 de abril (TOL8.422.408), que establece que las redes sociales, también pueden considerarse como un canal cerrado "*cuando adaptan su funcionalidad a un diálogo que excluye a terceros, participan, desde luego, de esa naturaleza*".

Con canales de comunicación cerrados[5] nos referimos a aquellos en los que se puede excluir la posibilidad de que un tercero entre[6]. Que el canal de comunicación sea cerrado es independiente de que el policía y los investigados estén utilizando un medio de transmisión público o privado, es decir, lo que caracteriza un canal de comunicación cerrado es la expectativa de secreto[7].

Como así establece la STS 249/2008, de 20 de mayo, estos canales "*se caracterizan por la expresa voluntad del comunicante de excluir a terceros del proceso de comunicación*"[8]. También destacamos la STC núm. 170/2013, de 7 octubre, que determina que ha de entenderse como canal cerrado de comunicación "*aquel en el que existe una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenida*"[9].

En un primer momento, en concreto en el Anteproyecto de reforma de la LECrim, se permitía que los AEV pudieran actuar a través de canales de comunicación abiertos[10], y que posteriormente pudiera mantener su identidad supuesta cuando fuera aceptado en canales cerrados de comunicación. Este hecho pronto suscitó grandes inconvenientes, el más grave, la falta de pronunciamiento acerca de la necesidad de autorización judicial para navegar a través de este tipo de canales de comunicación. No se entendía cómo se podía

[5] La doctrina ha conceptualizado y analizado este concepto, el de canal cerrado de comunicación en muchas ocasiones. Destacamos a: VALVERDE MEGÍAS, R. Medidas accesorias en los procedimientos por delito de abuso y explotación sexual de menores mediante tecnologías de la información y comunicación y relativos a la pornografía infantil. En *Estudios Jurídicos*. Madrid: Centro de Estudios Jurídicos, 2012. núm. 2012. p. 20; GONZÁLEZ LÓPEZ, J.J. Infiltración policial en Internet: algunas consideraciones. En *Revista del Poder Judicial.* Madrid: CGPJ, 2007. nº85. p. 8; CAROU GARCÍA, S. El agente encubierto como instrumento de lucha contra la pornografía infantil en internet: El guardián al otro lado del espejo. En *Cuadernos de la Guardia Civil, Revista de seguridad pública*. Madrid: Ministerio del Interior, 2018, núm. 56. p. 36.

[6] RIZO GÓMEZ, B. La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la ley 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. En ASENCIO MELLADO (Dir.); FERNÁNDEZ LÓPEZ, M. (Coord.), *Justicia y nuevas formas de delincuencia*. Valencia: Tirant lo Blanch, 2017. p. 103.

[7] FERNÁNDEZ RODRÍGUEZ, J.J. *Secreto de comunicaciones en internet*. Madrid: Civitas, 2004. p. 99.

[8] España. Tribunal Supremo. Sentencia núm. 249/2008, de 20 de mayo (TOL1.333.381).

[9] España. Tribunal Supremo. Sentencia núm. 170/2013, de 7 de octubre (TOL3.531.809).

[10] En concreto, en el apartado sexto del art. 282 bis del Anteproyecto, se establecía que "*Los funcionarios de la Policía Judicial podrán actuar con identidad supuesta en los canales de comunicación abiertos a una pluralidad indeterminada de personas para la detección y esclarecimiento de delitos que puedan ser cometidos por medios informáticos o a través de telecomunicaciones o servicios de comunicación. Cuando como consecuencia de la utilización de dicha identidad el funcionario sea aceptado en comunicaciones mantenidas en canales cerrados de comunicación, podrá seguir manteniendo la identidad supuesta…*".

utilizar una identidad supuesta o nombres falsos en canales de comunicación abiertos sin que fuera necesaria una autorización judicial.

Todo ello provocó un cambio en la redacción del proyecto y se estableció que solo sería necesaria la correspondiente autorización judicial cuando el AEV actuara a través de canales cerrados. Esto no quiere decir que los agentes de policía no puedan navegar a través de canales abiertos de comunicación, como hemos expuesto anteriormente, es una práctica habitual. En el caso del ciberpatrullaje, los agentes actúan tras un nombre falso o *nickname*, y en el caso de que sospechen de alguna persona, y crean que debe comenzar a ser investigado, entonces se iniciará el proceso para que se le proporcione una identidad supuesta y comenzará la verdadera infiltración. El agente ciberpatrullador no tiene que coincidir necesariamente con el agente que posteriormente se infiltre, pueden ser personas diferentes.

Otro de los asuntos que conllevó dudas al respecto por este motivo, fueron los programas P2P. Se trata de programas destinados a compartir archivos a través de la red y de internet de forma gratuita. Muchos han sido los programas P2P que han salido a la luz, como EMULE, *Napster* o *FreeNet*. En todos ellos los usuarios tenían la posibilidad de compartir archivos de diversas clases para que otros usuarios pudieran acceder a ellos de forma gratuita, y esto hacía que, por ejemplo, las discográficas, terminaran bajando sus precios en los cd, ya que los cibernautas comenzaron a consumir música, películas, series, etc. a través de estos sistemas.

Se lucha por proteger los derechos de autor que estos programas violan constantemente, pero lo cierto es que, en el mundo de internet, es muy difícil frenar este tipo de acciones, sobre todo en este tipo de intercambios de archivos en los que los usuarios son completamente anónimos.

El TS tuvo la oportunidad de referirse a este tipo de programas en la STS de 14 de julio de 2010, que versaba sobre un caso en el que el investigado se descargaba archivos a través de EMULE (programa P2P) cuyo contenido era pornografía infantil. Uno de los motivos de recurso fue el de vulneración del artículo 18.1 y 3 de la CE que garantiza el derecho de las comunicaciones. La sentencia establece que "*quien utiliza un programa P2P, en nuestro caso EMULE, asume que muchos de los datos se convierten en públicos para los usuarios de internet, circunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía, datos públicos en internet, no se hallaban protegidos por el art. 18.1º ni por el 18-3 C.E. (…) cuando las comunicación a través de la Red se establece mediante un programa P2P, como en el EMULE o EDONKEY, al que puede acceder cualquier usuario de aquélla, el operador asume que muchos de los datos que incorpora a la red pasen a ser de público conocimiento para cualquier usuario de Internet, como, por ejemplo el I.P., es decir, la huella de la entrada al programa, que queda registrada siempre (…)Por ello, no se precisa autorización judicial para conocer lo que es público, y esos datos legítimamente*

obtenidos por la Guardia Civil en cumplimiento de su obligación de persecución del delito y detención de los delincuentes, no se encuentran protegidos por el art.18.3 C.E.[11]".

Como podemos observar, los programas P2P son sistemas de comunicación abiertos, en los que el policía no tiene por qué tener una autorización judicial previa, pueden introducirse en estos medios sin necesidad de una identidad supuesta y de ser un AEV. Asimismo, en labores de ciberpatrullaje, los agentes de policía pueden vigilar canales de comunicación abiertos, pero en el momento en el que intentan entrar en un chat, foro, o conversación que requiera una contraseña, deberá pedir la correspondiente autorización judicial.

En definitiva, el AEV podrá actuar a través de canales de comunicación cerrados siempre y cuando lo haga amparado por una autorización judicial, ya que, de lo contrario, se vulnerarán ciertos derechos fundamentales, y esto sucede porque el usuario o investigado comparte sus datos personales, sus archivos y mantiene relaciones con el AEV en un contexto de secreto, de secreto respecto a terceros ajenos. Los datos personales que el investigado comparta podrán ser íntimos o sensibles, o datos personales que únicamente puedan identificar a una persona en concreto. Acceder a canales cerrados de comunicación es la principal misión del AEV, infiltrarse en estos canales, en la Deep Web, para poder conseguir información relevante sobre las acciones cometidas y las que se están cometiendo.

3. Límites a la actuación del agente encubierto virtual

3.1. Abrir cuentas corrientes y comerciar electrónicamente

La doctrina[12] considera que el AEV puede actuar en el tráfico socio-económico abriendo cuentas corrientes y comerciando electrónicamente, todo ello con la finalidad de investigar determinados delitos económicos.

En concordancia con esta perspectiva, en nuestra opinión, a pesar de que no viene establecido expresamente en el art. 282 bis de la LECrim, consideramos que el AEV podrá realizar estas actuaciones cuando lo que se persigan sean delitos que atenten al orden socio-económico. De hecho, creemos que sería muy aclaratorio en el futuro, que una reforma de la LECrim se incluyera esta posibilidad de forma explícita.

[11] España. Tribunal Supremo. Sentencia núm. 680/2010, de 14 de julio (TOL1.919.209).

[12] Autores como URIARTE VALIENTE L.M. (2012). El agente encubierto como medio de investigación de delitos de pornografía infantil en Internet. En *Estudios Jurídicos*. Madrid: Centro de Estudios Jurídicos, 2012, núm. 2012. pp. 13-14 o CLADERA ALBA, F., y GARCÍA MARTÍNEZ, G. Blanqueo de capitales y agente encubierto en Internet. En *Fodertics 5.0. Estudios sobre nuevas tecnologías y justicia*. Granada: Comares, 2016. p. 199, consideran que, en los casos de delitos económicos o patrimoniales, el Juez de Instrucción podrá autorizar la apertura de cuentas corrientes o comerciar electrónicamente.

Supone para el AEV una gran ventaja disponer de ciertos importes de dinero que le sirvan para demostrar capacidad económica y para realizar negocios ficticios. En palabras de DELGADO MARTÍN, el AEV deberá poder incluir en su ámbito de actuación actividades relacionadas con el comercio electrónico porque son "*necesarios para la cada vez más frecuente criminalidad a través de internet, no solamente en materia de pedofilia y pornografía infantil, sino también en fraudes económicos cometidos utilizando los instrumentos propios de la www*"[13].

3.2. Envío e intercambio de archivos ilícitos

El intercambio y envío de archivos ilícitos se recoge en el art. 282 bis de la LECrim, en concreto en su sexto apartado. Es una de las actividades propias del AEV siempre que exista autorización judicial específica para ello.

En el caso de operaciones encubiertas físicas, ya se permitía, por ejemplo, manejar, e incluso enviar, paquetes de drogas por parte del agente de policía. Toda la droga que se maneja por la policía está controlada, y se pretende en la medida de lo posible que no llegue a manos de delincuentes o a manos del consumidor. Este hecho, el de cometer ciertas actuaciones con el fin de parecer realmente un delincuente o un integrante de una banda o una organización, en el plano virtual se traduce en el envío de archivos ilícitos. Este tipo de prácticas se admiten porque lo que se pretende es que consideren al agente infiltrado como uno más.

Esta capacidad, la de poder enviar archivos ilícitos, es una de las que diferencia al AEV de un agente de policía ordinario, y es que este último, ocultará en muchas operaciones u ocasiones su condición de policía, pero no podrá enviar material ilegal como sí lo puede hacer el AEV con autorización específica.

3.2.1. Necesidad de autorización específica

La norma exige, de forma expresa, una autorización específica para el envío o intercambio de archivos ilícitos por parte del AEV. Esta autorización podrá estar incluida en resolución judicial autorizante, o en otra separada que se dicte posteriormente. Lo importante, es que se autorice expresamente que puede hacerlo.

Es muy importante que exista un control judicial sobre estas actuaciones, ya que incorporar a internet archivos de contenido ilícito puede poner en riesgo determinados bienes jurídicos, como, por ejemplo, la lesión a la integridad moral de la víctima en los casos en los que el archivo ilícito contenga imágenes pornográficas de menores de edad.

[13] DELGADO MARTÍN, J. El proceso penal ante la criminalidad organizada. El agente encubierto. En PICO I JUNOY, J. (dir.), *Problemas actuales de la justicia penal*. Barcelona: Bosch, 2001. p. 39.

Por este motivo, deberá ser autorizado de forma individualizada. Con ello lo que se pretende es que el Juez pueda valorar casos por caso, analizando si se respetan los criterios de necesidad, adecuación y proporcionalidad[14]. Asimismo, señala TEJADA DE LA FUENTE, que "*no pueden quedar al margen de esa valoración aspectos tales como el tipo de archivo ilícito que se pretende intercambiar o enviar; el destino de esos archivos y el control que pueda establecerse sobre el movimiento de los mismos en la red tanto en orden a la posibilidad de su posterior recuperación como para conjurar el riesgo de provocación delictiva*"[15].

En cuanto a la necesidad o no de una autorización judicial previa para poder enviar archivos ilícitos, en un primer momento surgían dudas, pero debido a la polémica que existió cuando se publicó el Anteproyecto de Ley Orgánica, basada en que fuera el Policía Judicial quien tomara esa decisión, finalmente se optó por lo que hoy en día está regulado en la Ley. En concreto, el Consejo Fiscal, en el Informe al Proyecto de reforma de la LECrim, puso de relieve la peligrosidad que entrañaba que un policía judicial pudiera enviar archivos ilícitos sin una resolución judicial previa, ya que podría violar determinados derechos fundamentales.

Hay que estudiar qué tipo de archivos se pretende enviar, y a quién, es decir el destinatario, y, además, qué control posterior va a existir sobre estos archivos y su movimiento en la red, ya que es cuanto menos peligroso que determinados archivos con contenido ilícito se difundan por la red.

En nuestra opinión, la regulación actual es acertada, creemos que lo más correcto es que deba existir una autorización judicial previa antes del envío de un archivo ilícito. Esta actuación puede autorizarse en el momento en que se ve necesario para los fines de la investigación, surgiendo dicha necesidad, durante el desarrollo del operativo; o bien, en un momento posterior. En el caso de que esté dispuesta en la primera autorización, esta actuación debe contar con una motivación específica y separada de aquella que explica el razonamiento para autorizar la investigación mediante AEV. Si se autoriza en un momento posterior, deberá estar también motivado de forma expresa.

Así, este tipo de actuación no puede quedar amparado por la autorización judicial general que autoriza al AEV a actuar ordinariamente, y esto es debido a que el intercambio de este tipo de archivos entraña un plus de peligrosidad. En palabras de RIZO GÓMEZ, "*se trata de un plus, algo que debe ser adicional a la*

[14] Algunos autores como CAROU GARCÍA S., referencia 5, p. 37, consideran que, incluso, se podría habilitar a la policía a que llevaran a cabo este tipo de actuaciones, y, posteriormente, se produzca el control judicial.

[15] TEJADA DE LA FUENTE, E. Aproximación a las herramientas de investigación tecnológica en el Proyecto de reforma procesal. En *Jornada sobre violencia de género: aspectos prácticos con especial referencia a las nuevas tecnologías*, Madrid: Centro de Estudios Jurídicos, 2015. p. 13.

actuación del agente encubierto en Internet, a pesar de que en ocasiones la propia circulación se vuelva imprescindible al objeto de asegurar el éxito de la investigación penal" [16].

La correspondiente autorización judicial, deberá manifestar las circunstancias que han servido para aprobar la medida, y esta justificación deberá basarse en los principios de idoneidad, excepcionalidad y proporcionalidad.

Además, es importante que el intercambio de archivos ilícitos esté aprobado por una resolución judicial previa porque de esta forma podremos diferenciar este tipo de actuación con el ya analizado delito provocado[17–18]. El AEV no va a provocar el delito con el envío de archivos, sino que se sirve de esta posibilidad para avanzar en la investigación[19], y lo hace con todas las garantías. Con una resolución judicial por la cual se autoriza el intercambio de archivos de contenido ilícito, junto con la existencia de una previa relación entre el AEV y el investigado, no se podrá pensar que existe un delito provocado.

El AEV se infiltrará en un grupo de personas o interactuará con una persona en concreto, y es habitual que quien se encuentra al otro lado de la pantalla le pida identificarse como persona nueva a la que está conociendo o como nuevo miembro del grupo al que se quiere unir. Es muy habitual también que se le pida intercambiar, con él o con el resto del grupo, archivos que demuestren que está en sintonía con el resto, con los intereses del grupo o de la persona en concreto.

3.2.2. Acción

La norma señala que el AEV puede realizar dos tipos de acciones: envío e intercambio. Podrá enviar archivos ilícitos sin recibir material a cambio por parte del investigado, o podrá realizar un intercambio de material.

Es cierto que no se prevé expresamente que el AEV pueda únicamente recibir material ilícito, pero, en nuestra opinión, al poder enviar, actuación que entraña más riesgos, podrá también recibir[20]. Tampoco se prevé nada acerca de

[16] RIZO GÓMEZ, B., referencia 6, p. 118.

[17] LÓPEZ GARCÍA, E. Agente encubierto y agente provocador, ¿dos figuras incompatibles? En *Revista La Ley*. Madrid: Wolters Kluwer España, julio 2003, año XXIV núm. 5822. p. 2

[18] Según la STS 601/2000, de 14 de julio (TOL4.924.803), el delito provocado es *"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, delito que de no ser por tal provocación no se hubiere producido"*.

[19] URIARTE VALIENTE, L.M., referencia 12.

[20] España. Tribunal Supremo. Sentencia núm. 767/2007, de 3 de octubre (TOL1.156.511).

la compra de archivos, aunque puede incluirse en el concepto de "intercambio", pero en vez de material por material, de material por precio.

3.2.3. Contenido de los archivos ilícitos

En primer lugar, debemos analizar qué archivos ilícitos puede intercambiarse el AEV con el investigado, ya que podrán ser desde imágenes con contenido pornográfico infantil, hasta un software con un ejecutable orientado a ayudar en una investigación. El AEV podrá enviar aquellos archivos que puedan servir en el seno de la investigación, siempre y cuando tenga autorización expresa del órgano judicial, que tendrá que conocer el contenido de dicho archivo antes de autorizarlo. Cuando el archivo que se envía es, por ejemplo, un troyano[21], el órgano judicial, además, debe autorizar la realización de otra medida de investigación, como es el registro remoto de dispositivos.

Un archivo ilícito puede tener diversas finalidades, como, por ejemplo, enviar un programa que monitorice las pulsaciones del teclado del investigado o que siga sus acciones en la red. En el caso de que un AEV envíe este tipo de archivos, deberá contar con una autorización judicial expresa.

El intercambio o envío de archivos ilícitos por parte del AEV constituye una medida necesaria en su actuación para poder luchar contra los ciberdelitos, podemos apreciar esta importancia, por ejemplo, en los delitos de pornografía infantil[22], en los que los ciberdelincuentes suelen confiar en otras personas cuando se produce un intercambio de material pornográfico. Esta forma de actuar ha cambiado con el paso del tiempo, y los delincuentes cada vez más actúan en canales cerrados de comunicación como chats privados, y los policías tienen un acceso mucho más restringido. En estos casos, que el AEV pueda enviar archivos como si de un delincuente se tratara, es primordial para ganarse la confianza[23] de la persona que se encuentra detrás de la pantalla.

3.2.3.a. Archivos ilícitos que contienen pornografía infantil

El AEV es una figura controvertida y que suscita muchas dudas, pero uno de los aspectos más controvertidos es la posibilidad que existe de que pueda intercambiarse con los presuntos ciberdelincuentes material de contenido ilícito.

[21] El AEV, con autorización expresa para ello, podrá enviar un archivo con contenido sexual infantil, y este envío se utiliza para hacer el registro remoto de ordenadores, es decir, con el archivo se envía un troyano. El investigado ejecuta el archivo y el AEV automáticamente capta todo lo que contiene el ordenador.

[22] DE LA ROSA CORTINA, J.M. Delitos de pornografía infantil: otra vuelta de tuerca. En *Diario La Ley*. Madrid: Wolters Kluwer, 2012, núm. 7817.

[23] SALOM CLOTET, J. Pornografía infantil en la Red y su investigación. En *Estudios jurídicos*. Madrid: Centro de Estudios Jurídicos, 2007. pp. 2-3.

Este material que se envía al investigado suele contener en muchas ocasiones material pornográfico que tienen como protagonistas a menores de edad.

Es evidente que, si estos archivos o imágenes las creara el Estado o la policía, estarían incurriendo en la comisión de un delito tipificado[24], es decir, la creación de material pornográfico en el que intervienen menores de edad supone un delito. Por lo tanto, los archivos que se utilizan deben estar elaborados previamente por delincuentes. También podrá haberlos creado la policía, pero en este caso, en ellos los protagonistas no serán verdaderos menores de edad.

Ambas posibilidades doctrinales conllevan determinados problemas: En primer lugar, nos encontramos ante la opción de recurrir a archivos que la policía ha incautado en anteriores operaciones. Si se opta por esta posibilidad, siempre se deben respetar los principios de proporcionalidad, necesidad y excepcionalidad. Debemos tener en cuenta que utilizar material que han elaborado determinados pedófilos, y que ha sido incautado por la policía anteriormente, no deja de ser un supuesto en el que los archivos tienen como protagonistas a menores de edad reales.

Desde nuestro punto de vista, con esta actuación se va a dañar la imagen al menor y se están violando ciertos derechos fundamentales del mismo, como, por ejemplo, el de la intimidad y el derecho a la propia imagen. Si el sistema es garantista de cara al investigado, también debe serlo con la víctima, no podemos olvidarnos de esta y de sus derechos.

En segundo lugar, existe la posibilidad de elaborar material pornográfico ad hoc, es decir, elaborar archivos que sirvan concretamente para enviar a los investigados y que contengan imágenes de actores que son mayores de edad pero que por su físico pueden hacerse pasar por menores de edad[25].

Ahora bien, existe un problema si se opta por esta opción, ya que el investigado, en una fase posterior del proceso, cuando descubra o sospeche que las imágenes son protagonizadas por mayores de edad, podrá argumentar que era conocedor de ello, que sabía que aparentemente parecían niños pero que en realidad no se trataba de menores de edad, aunque tuvieran una apariencia infantil, incluso podría alegar que estaba confundido con la edad de los protagonistas[26].

---

[24] RODRÍGUEZ CARO, M.V. La infiltración policial: en el límite del Estado de Derecho. El inminente agente encubierto informático. En *Noticias Jurídicas*. 2015, Madrid. Disponible en: https://noticias.juridicas.com/conocimiento/articulos-doctrinales/10222-la-infiltracion-policial:-en-el-limite-del-estado-de-derecho-el-inminente-agente-encubierto-informatico/

[25] En este sentido BUENO DE MATA, F. (2012). Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿Deberían ampliarse las actuales funciones del agente encubierto en Internet? Obra colectiva *El proceso penal en la sociedad de la información, las nuevas tecnologías para investigar y probar el delito*. Madrid: La Ley, 2012. pp. 251-252, que entiende esta posibilidad como única.

[26] En este sentido destacamos a CAROU GARCÍA S., referencia 5, p.36.

Por supuesto, si se utiliza la opción de crear contenido pornográfico con actores y actrices que simulen ser menores de edad, lo correcto es que los actores y actrices que aparezcan en esas imágenes lo hagan voluntariamente y como parte de un trabajo remunerado, es decir, que sean contratados legalmente para el objetivo que se pretende conseguir.

También existe la posibilidad de crear archivos con programas informáticos que lo permitan, que sean capaces de elaborar vídeos o fotografías con menores de edad que no existen en la realidad[27]. Nos referimos a la elaboración de vídeos e imágenes retocados por ordenador, utilizando técnicas de inteligencia artificial. Este método es conocido como *deepfake*, y es capaz de elaborar vídeos de una persona haciendo algo que nunca ha hecho.

El *deepfake* es un modelo computacional que se basa en la tecnología *Deep learning* (inteligencia artificial), y las imágenes que se generan lo hacen matemáticamente mediante algoritmos a partir de fotos y vídeos de la persona que se quiere recrear.

De esta forma, en la imágenes y archivos ilícitos que el AEV intercambia, no habría menores de edad reales y realizando actos reales, sino que podría elaborarse un perfil de un menor ficticio y darle vida con este tipo de programa informático. Los *deepfakes* son técnicas de inteligencia artificial relativamente recientes y creemos que es una gran solución, ya que, además, nos estaríamos aprovechando de la progresión en el campo de la inteligencia artificial[28].

En nuestra opinión, consideramos que lo mejor es optar por esta segunda opción a pesar de que exista el problema expuesto. No podemos limitar los derechos fundamentales de los menores de edad a pesar de la gravedad o envergadura del delito que se está cometiendo. Debemos ser conscientes de que los menores de edad que aparecen en determinadas imágenes existen, y que crecerán, y se harán mayores de edad, y que les habrán sido limitados sus derechos fundamentales.

---

[27] GARCÍA CALDERÓN J.M. Algunas notas sobre la investigación del delito y la proporcionalidad. Curso de formación continua de fiscales *Jornadas de especialización en materia de criminalidad informática. Cibercrimen y Ciberterrorismo*. Madrid: Centro de Estudios Jurídicos, 2006. p. 18.

[28] MARTÍN RÍOS, M ª. DEL P. y VILLEGAS DELGADO, C. *El derecho en la encrucijada tecnológica. Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial*. Valencia: Tirant lo Blanch, 2022.

3.2.3.b. Archivos ilícitos con material distinto al de pornografía infantil

Además de archivos con contenido pornográfico infantil, el AEV podrá enviar e intercambiar otro tipo de material ilícito, nos referimos a los programas informáticos maliciosos, como, por ejemplo, los troyanos y *spyware*[29].

Asimismo, el AEV podrá enviar manuales de elaboración de armas y explosivos, propaganda *yihadista*… todo aquel material necesario que le ayude a asentar y reforzar su falsa identidad.

3.3. Análisis de algoritmos asociados a los archivos ilícitos

Como hemos expuesto, el AEV puede enviar material ilícito si sospecha que la persona con la que está manteniendo una conversación está cometiendo un delito, y estos archivos podrán ser encontrados posteriormente en un ordenador en el seno de una intervención policial domiciliaria. Se plantea el problema de que, por lo general en delitos relacionados con la pornografía infantil, el AEV tiene que mandar material ilícito para demostrar que está en la misma sintonía que la persona investigada. En ocasiones incluso es obligatorio para el AEV mandar este tipo de material para ser aceptado en un foro en concreto, y, por tanto, si no se hace, la investigación podría fracasar.

Ante este tipo de situaciones, se debe controlar la incorporación a la red de material ilícito. El apartado 6 del artículo 282 bis de la LECrim recoge la posibilidad de "*analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos*". Con esta posibilidad se pueden analizar e identificar los archivos que se interceptan[30].

Lo que interesa es el resultado de los algoritmos, ya que con ello se podrán identificar los archivos informáticos intercambiados. Según RUBIO ALAMILLO, lo importante es averiguar la clave alfanumérica de los archivos, denominado también como el *hash*, definido por el citado autor como un "*código alfanumérico*

[29] ZARAGOZA TEJADA, J.I. *La modificación operada por la Ley 13/2015. El agente encubierto informático.* Curso de formación continua, Madrid: Centro de Estudios Jurídicos, 2016. p. 23.

[30] En palabras de VELASCO NÚÑEZ, E. *Posición del Instructor ante la petición de investigación de desarrollo de medidas de investigación restrictivas de derechos*. En curso de formación descentralizada de jueces y magistrados. Madrid: CGPJ, 2016, Cuadernos Digitales de Formación nº56. p. 65, "*siguiendo la secuencia serial del algoritmo hash del contenido del envío telemático se puede descubrir a quién más se ha enviado, y en consecuencia, quién puede ser connivente en el envío de material presuntamente delictivo, piénsese, por ejemplo el análisis del hash de un archivo pretendiendo la captación, adoctrinamiento o adiestramiento terroristas; igualmente por esta vía se podría, con la habilitación reforzada judicial, analizar las modificaciones operadas en la secuenciación algorítmica del hash de ficheros o envío, o la realizada sobre sus porcentajes de píxeles, que en envíos semejantes, también pueden ayudar a descubrir ciertas actividades delictivas*".

obtenido mediante un procedimiento matemático, el cual es único para el fichero, disco o memoria del cual se calcula"[31].

Es cierto que el legislador no ha sido muy conciso a la hora de definir a qué se refiere con "algoritmo", ya que si nos basamos en la definición de la Real Academia Española (RAE), podemos definirlo como "*conjunto ordenado y finito de operaciones que permite hallar la solución de un problema*"[32], y en realidad, a lo que nos referimos, no es exactamente a este concepto de algoritmo, sino a una identificación alfanumérica que nos permita identificar cada uno de los archivos ilícitos, por decirlo de otra forma, es como si estuviéramos buscando el DNI del archivo.

Al fin y al cabo, lo que se pretende es poder identificar los archivos ilícitos, y por esta razón lo que nos interesa es el *hash*. Así lo expresa también la Fiscalía en el Informe del Consejo Fiscal al Anteproyecto, que además de hacer mención al *hash*, hace mención al término de algoritmo, estableciendo que "*el término algoritmo se emplea para definir los pasos e instrumentos necesarios para obtener un resultado como es precisamente el hash*" y añade que lo que pretende el Anteproyecto es "*referirse a la posibilidad de identificar inequívocamente los archivos ilícitos que se hayan enviado o intercambiado, por lo cual lo importante a esos efectos no es el análisis de los algoritmos sino el análisis de los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos*"[33].

La identificación alfanumérica o *hash* es de vital importancia para no perder la pista de los archivos ilícitos, para poder conocer el recorrido que hacen y poder tenerlos localizados, y, sobre todo, para tener conocimiento de si este material ha sido introducido por el AEV o por el delincuente. Como fin último, poder localizar mediante algoritmos los archivos ilícitos que se introducen en la red, es el de poder localizarlos una vez han hecho su función y poder eliminarlos.

Los archivos que el AEV utiliza en su infiltración, en nuestra opinión, deberán estar registrados en informes periciales o inventarios que los recoja como material ilícito elaborado o intercambiado como objeto de una infiltración, es decir, si en una investigación policial se descubren archivos ilícitos que posteriormente se van a utilizar en una investigación encubierta, estos archivos deben estar recogidos en un inventario o base de datos segura que incluya

[31] RUBIO ALAMILLO, J. La informática en la reforma de la Ley de Enjuiciamiento Criminal. En Diario La Ley, diciembre 2015, Madrid. Disponible en: https://peritoinformaticocolegiado.es/blog/la-informatica-en-la-reforma-de-la-ley-de-enjuiciamiento-criminal/.

[32] Definición que da la Real Academia Española del concepto de algoritmo, disponible en: https://dle.rae.es/algoritmo

[33] Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica de Modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas, Madrid, 23 de enero de 2015, pp. 26-27.

también el *hash* de cada archivo (y así no se podrán manipular posteriormente). Esta posibilidad existe porque "*no sería posible distinguirlos del material ilícito realmente obtenido por el acusado sin la ayuda policial*"[34].

Es muy importante que los archivos que reciben los investigados o posibles delincuentes por parte del AEV puedan ser fácilmente identificados posteriormente, porque los ciberdelincuentes pueden enviarlos nuevamente a otros usuarios y podrán ser distribuidos por la red sin control. Es crucial que la Policía Judicial sepa reconocer los archivos que han servido como señuelos y sepan separarlos de los archivos que son verdaderamente ilícitos y han sido elaborados por delincuentes reales.

Imaginemos la situación en la que un AEV envía archivos ilícitos a un investigado. Si el investigado resulta culpable, no existe ningún problema, pero si posteriormente resulta inocente y pasa un plazo de tiempo, y esta persona, por cualquier otra razón, sufre una redada policial en su casa o un registro domiciliario, y los policías descubren en su ordenador los archivos ilícitos que previamente han sido enviados por el AEV, nos encontraríamos ante un problema. Si no somos capaces de identificar si estos archivos han sido elaborados por la policía o por el investigado, las consecuencias que pueden acarrear para el investigado pueden ser devastadoras.

3.4. Interacción física entre el agente encubierto virtual y el investigado

El artículo 282 bis, apartado 7 de la LECrim, establece que, en el curso de la investigación, el juez competente podrá autorizar al AEV a que mantenga encuentros físicos con el investigado. Para ello, también es necesario que exista una resolución autorizante específica. Estos encuentros pueden provocar o pueden causar otro tipo de actuaciones:

3.4.1. Reuniones físicas entre el agente encubierto virtual y el investigado

El primer problema que se plantea es el de si es necesaria una nueva autorización en los casos en los que se sale del mundo virtual y se llega al mundo real.

Este tipo de reuniones físicas deben estar previstas en la autorización judicial inicial, y si no, deberá dictarse de forma específica, y esto, por varios motivos. En primer lugar, porque en la autorización deberá establecerse la identidad ficticia no cibernética del agente de policía, y se le deberá facultar a portar determinados instrumentos u objetos (por ejemplo, armas). Esta facultad,

[34] RUBIO ALAMILLO, J., referencia 31.

la de utilizar determinados instrumentos, es diferente a la facultad que tiene el AEV para utilizar herramientas virtuales[35].

Otro de los problemas que surge en este tipo de reuniones, es el ámbito de actuación, ya que los delitos que investiga el AEV no son los mismos que investiga un Agente Encubierto Físico (en adelante, AEF). Algunas de las actividades delictivas investigadas por el AEV no están permitidas en la investigación del AEF. Por ello, nos resulta inviable que se active a un AEF para acudir a determinadas reuniones, ya que su ámbito de actuación se verá encorsetado por los requisitos que deben cumplirse (que el delito esté siendo cometido por una organización criminal en todo caso).

En nuestra opinión, por los motivos expuestos, siempre es necesaria una autorización específica con motivación expresa, venga contenida en la autorización inicial o en una posterior.

3.4.2. Obtención de imágenes y grabación de conversaciones en encuentros previstos entre el agente encubierto virtual y el investigado

El juez competente, y así viene regulado en el art. 282 bis, apartado 7, de la LECrim, podrá autorizar que el AEV obtenga imágenes y grabe las conversaciones que se mantienen en los encuentros que se produzcan entre este y el investigado[36]. El legislador ha dado la posibilidad de que estas grabaciones se puedan llevar a cabo incluso cuando los encuentros se producen dentro de un domicilio[37].

Para este tipo de actuación, el AEV tendrá que obtener una nueva autorización judicial[38], y no valdrá con la resolución judicial inicial que ampara la actuación del AEV. Esto se debe a que este tipo de actuación, el de obtención de imágenes y grabación de conversaciones, limita determinados derechos fundamentales del investigado que en un primer momento no estaban siendo limitados. Podríamos definir estas actuaciones como adicionales, que surgen en el transcurso de una infiltración, que no se autorizan en un primer momento porque ni siquiera se sabe si se van a dar o no.

---

[35] VELASCO NÚÑEZ, E., referencia 30, p. 65.

[36] Así se establece también en el Anteproyecto de la LECrim del año 2020, en concreto, en su artículo 513: *"si en el curso de la investigación resultase necesario para asegurar la fuente de prueba, el Juez de Garantías, a instancia del Ministerio Fiscal, podrá acordar que la autorización se entienda a la grabación y obtención de imágenes de las comunicaciones entre el agente encubierto y la persona investigada. El fiscal informará al Juez de Garantías, en la forma en que este disponga, sobre el desarrollo y los resultados de la medida*".

[37] VELASCO NÚÑEZ, E., referencia 30, p. 64

[38] Sobre la habilitación para grabar la imagen o el sonido en el curso de sus actuaciones, destacamos a SERRANO GARCÍA M.J. La regulación de los medios de investigación tecnológica. En curso de formación continua de fiscales *Jornadas de especialistas de la jurisdicción militar*, Madrid: Centro de Estudios Jurídicos, 2018. pp. 55-56.

Si en el transcurso de una infiltración en internet, el AEV considera que se precisan actuaciones adicionales, este deberá solicitar una autorización judicial concreta y el órgano competente deberá valorar si es necesario o no, en definitiva, deberá valorar la viabilidad de la actuación solicitada.

Esta valoración por parte del órgano competente deberá estar motivada y se deberán prestar especial atención a los principios de idoneidad y necesidad de la medida, pero, sobre todo, se deberá prestar atención al principio de proporcionalidad. Se deberá estudiar y analizar si la obtención de imágenes y grabación de conversaciones solicitada es necesaria e idónea para obtener cierta información, si no existe otro tipo de actuación menos lesiva de derechos fundamentales y si es proporcional realizar estas actuaciones con el fin perseguido y los delitos que se están investigando.

En cuanto a la regulación que debemos atender en cuanto a la grabación de imágenes y sonido, al no estar regulado específicamente en materia de AEV, debemos guiarnos por lo dispuesto en la Ley 13/2015, Capítulo VI, Título VIII, sobre "Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos".

3.4.3. Comunicaciones telefónicas entre el agente encubierto virtual y el investigado

En el curso de una infiltración virtual, en la que el AEV mantiene relación con el investigado en canales de comunicación cerrados, podrá darse la posibilidad de que este, le proponga mantener una conversación telefónica. En estos casos, nos planteamos la misma cuestión, la de si es necesaria una autorización específica para ello.

ZARAGOZA TEJADA[39] examina este escenario, y considera innecesario que se emita una nueva autorización judicial específica, en su opinión "*dictar otra resolución judicial para mantener este tipo de contactos es claramente redundante*". Una vez conseguida la autorización judicial habilitante, el AEV podría estar facultado también para realizar otro tipo de actos, siempre y cuando no se produjera una intromisión en el derecho al secreto de la comunicaciones, en el de intimidad o el derecho a la inviolabilidad del domicilio, entre otros, ya que "*estos contactos telefónicos quedaban enmarcados dentro del ámbito de la investigación ya autorizada al dictar la resolución judicial de habilitación para actuar como agente encubierto online*".

En nuestra opinión, a pesar de que estamos de acuerdo en que este tipo de actuaciones pueden quedar enmarcadas en esta primera habilitación legal, consideramos que, según el tenor literal del art. 282 bis, apartado 7, el AEV solo está habilitado, en principio, para actuar a través de chats o foros privados en internet, por tanto, para realizar actuaciones que se dan en el mundo físico o en

[39] ZARAGOZA TEJADA, J.I., referencia 29, pp. 28-29.

el mundo real, no en el informático, será necesaria la correspondiente resolución judicial adicional. Asimismo, en la mayoría de las ocasiones, estas conversaciones serán grabadas, y es estrictamente necesaria la autorización judicial para ello, y así viene establecido en la Ley[40]. Para la grabación de las conversaciones que se puedan dar, es necesaria una autorización judicial expresa, y ello, aunque se hagan en el mundo virtual.

4. Bibliografía

BUENO DE MATA, F. (2012). Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿Deberían ampliarse las actuales funciones del agente encubierto en Internet? Obra colectiva *El proceso penal en la sociedad de la información, las nuevas tecnologías para investigar y probar el delito*. Madrid: La Ley, 2012.

CAROU GARCÍA, S. El agente encubierto como instrumento de lucha contra la pornografía infantil en internet: El guardián al otro lado del espejo. En *Cuadernos de la Guardia Civil, Revista de seguridad pública*. Madrid: Ministerio del Interior, 2018, núm. 56.

CLADERA ALBA, F., y GARCÍA MARTÍNEZ, G. Blanqueo de capitales y agente encubierto en Internet. En *Fodertics 5.0. Estudios sobre nuevas tecnologías y justicia*. Granada: Comares, 2016.

DE LA ROSA CORTINA, J.M. Delitos de pornografía infantil: otra vuelta de tuerca. En *Diario La Ley.* Madrid: Wolters Kluwer, 2012, núm. 7817.

DELGADO MARTÍN, J. El proceso penal ante la criminalidad organizada. El agente encubierto. En PICO I JUNOY, J. (dir.), *Problemas actuales de la justicia penal*. Barcelona: Bosch, 2001.

FERNÁNDEZ RODRÍGUEZ, J.J. *Secreto de comunicaciones en internet*. Madrid: Civitas, 2004.

GARCÍA CALDERÓN J.M. Algunas notas sobre la investigación del delito y la proporcionalidad. Curso de formación continua de fiscales *Jornadas de especialización en materia de criminalidad informática. Cibercrimen y Ciberterrorismo*. Madrid: Centro de Estudios Jurídicos, 2006.

GONZÁLEZ LÓPEZ, J.J. Infiltración policial en Internet: algunas consideraciones. En *Revista del Poder Judicial.* Madrid: CGPJ, 2007. nº85.

LÓPEZ GARCÍA, E. Agente encubierto y agente provocador, ¿dos figuras incompatibles? En *Revista La Ley.* Madrid: Wolters Kluwer España, julio 2003, año XXIV núm. 5822.

MARTÍN RÍOS, M ª. DEL P. y VILLEGAS DELGADO, C. *El derecho en la encrucijada tecnológica. Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial*. Valencia: Tirant lo Blanch, 2022.

[40] Artículo 588 quarter a. de la LECrim

RIZO GÓMEZ, B. La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la ley 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. En ASENCIO MELLADO (Dir.); FERNÁNDEZ LÓPEZ, M. (Coord.), *Justicia y nuevas formas de delincuencia*. Valencia: Tirant lo Blanch, 2017.

RODRÍGUEZ CARO, M.V. La infiltración policial: en el límite del Estado de Derecho. El inminente agente encubierto informático. En *Noticias Jurídicas*. 2015, Madrid. Disponible en: https://noticias.juridicas.com/conocimiento/articulos-doctrinales/10222-la-infiltracion-policial:-en-el-limite-del-estado-de-derecho-el-inminente-agente-encubierto-informatico/

RUBIO ALAMILLO, J. La informática en la reforma de la Ley de Enjuiciamiento Criminal. En Diario La Ley, diciembre 2015, Madrid. Disponible en: https://peritoinformaticocolegiado.es/blog/la-informatica-en-la-reforma-de-la-ley-de-enjuiciamiento-criminal/

SALOM CLOTET, J. Pornografía infantil en la Red y su investigación. En *Estudios jurídicos*. Madrid: Centro de Estudios Jurídicos, 2007.

SERRANO GARCÍA M.J. La regulación de los medios de investigación tecnológica. En curso de formación continua de fiscales *Jornadas de especialistas de la jurisdicción militar*, Madrid: Centro de Estudios Jurídicos, 2018.

TEJADA DE LA FUENTE, E. Aproximación a las herramientas de investigación tecnológica en el Proyecto de reforma procesal. En *Jornada sobre violencia de género: aspectos prácticos con especial referencia a las nuevas tecnologías*, Madrid: Centro de Estudios Jurídicos, 2015.

URIARTE VALIENTE L.M. (2012). El agente encubierto como medio de investigación de delitos de pornografía infantil en Internet. En *Estudios Jurídicos*. Madrid: Centro de Estudios Jurídicos, 2012, núm. 2012.

VALVERDE MEGÍAS, R. Medidas accesorias en los procedimientos por delito de abuso y explotación sexual de menores mediante tecnologías de la información y comunicación y relativos a la pornografía infantil. En *Estudios Jurídicos*. Madrid: Centro de Estudios Jurídicos, 2012. núm. 2012.

VELASCO NÚÑEZ, E. *Posición del Instructor ante la petición de investigación de desarrollo de medidas de investigación restrictivas de derechos*. En curso de formación descentralizada de jueces y magistrados. Madrid: CGPJ, 2016, Cuadernos Digitales de Formación nº56.

ZARAGOZA TEJADA, J.I. *La modificación operada por la Ley 13/2015. El agente encubierto informático.* Curso de formación continua, Madrid: Centro de Estudios Jurídicos, 2016.

Conflicto de intereses
El autor declara no tener ningún conflicto de intereses.

Financiación
El documento ha sido elaborado sin financiación.