EL AGENTE ENCUBIERTO INFORMÁTICO A EXAMEN: UN ANÁLISIS DE SU REGULACIÓN Y DE LA VALIDEZ DE SU ACTIVIDAD INVESTIGADORA Y PROBATORIA EN EL PROCESO PENAL.

Dr. Saúl González García.

Profesor Sustituto Interino Departamento

Derecho Procesal de la Universidad de Granada

RESUMEN

En el presente trabajo analizamos detalladamente la regulación del agente encubierto informático y abordamos, desde un punto de vista práctico, los recientes pronunciamientos del Tribunal Supremo en relación con los requisitos para la validez de la prueba obtenida por esta diligencia de investigación así como las condiciones para su válida incorporación como prueba de cargo al proceso penal para concluir con una valoración sobre esta figura, señalando aquellas cuestiones que deben de ser abordadas por el Legislador a fin de completar su parca regulación.

ABSTRACT

In this paper we analyze in detail the regulation of the undercover computer agent and we approach from a practical point of view the recent pronouncements of the Supreme Court in relation to the requirements for the validity of the evidence obtained by this investigation as well as the conditions for its valid incorporation as proof of charge to the penal process to conclude with an appraisal on this investigation diligence and pointing out those questions that should be addressed by the Legislator in order to complete his limited regulation.

PALABRAS CLAVE

Agente encubierto informático, prueba nula, canal cerrado de comunicaciones, delito provocado.

KEY WORDS

Undercover computer agent, null evidence, closed communications channel, offense induce.

# Introducción.

La criminalidad organizada ha encontrado en las nuevas tecnologías un verdadero filón y cada vez nos encontramos con mayor cantidad, o bien de delitos informáticos, o bien de delitos tradicionales que emplean las TIC como un medio idóneo para lograr la consumación del delito.

En las antípodas de los principios y finalidades que inspiraron la creación de Internet, éste se ha convertido en una herramienta fundamental para nuevas fórmulas de criminalidad cuyo aumento es alarmante. En este sentido las cifras del Ministerio del Interior no dejan lugar a dudas sobre el aumento exponencial del cibercrimen en nuestro país. Por ilustrar esta cuestión, podemos señalar que los fraudes informáticos se han multiplicado por 3 desde 2011 hasta 2017 pasando de 20.000 a 60.000 y que los delitos sexuales cometidos a través de internet prácticamente se han duplicado en el referido periodo pasando de los 700 a los 1.300.[[1]](#footnote-2)

Algunas de las amenazas más graves que se ciernen sobre nuestra sociedad revisten la fórmula de un código binario de unos y ceros sobre el que se construye toda la sociedad de las Tecnologías de la Información y Comunicación (TIC). Resulta, cuando menos curioso, que algo de apariencia inofensiva como un código binario de lugar a la comisión de crímenes tan execrables como la pornografía infantil, el enaltecimiento del terrorismo o que pueda atentar contra el derecho fundamental al honor o la intimidad con tal virulencia que sean imposibles de restablecerse.

En semejante escenario de cibercrimen, nuestro Estado de Derecho necesita dotarse de mecanismos que permitan luchar frente a éste de forma efectiva. Estos mecanismos deben de orientarse tanto a la prevención de los delitos como a su persecución una vez consumados. En esta lucha, y especialmente en la función represora, el Estado necesita incluir en su ordenamiento procesal medios de investigación idóneos que, dando cumplimiento a los principios y garantías constitucionales que informan nuestro ordenamiento procesal, permitan llevar a cabo una labor investigadora que obtenga como resultado pruebas de la actividad ilícita que puedan sustentar el posterior ejercicio de la acción penal contra los ciberdelincuentes.

En este contexto la figura del agente encubierto informático se revela como uno de los medios de lucha contra el cibercrimen más idóneo junto con las denominadas diligencias de investigación tecnológicas, introducidos, todos ellos, en la reforma de la LECRIM llevada a cabo por 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. Esta necesidad de dotarse de nuevos medios de lucha contra la cibercriminalidad la apunta el propio Legislador en la Exposición de Motivos de la citada norma cuando señala que las nuevas tecnologías han puesto de manifiesto la insuficiencia de un cuadro normativo concebido para tiempos bien distintos.

# El agente encubierto informático, una pieza clave en la investigación del cibercrimen.

# La relevancia del agente encubierto informático en la determinación del objeto del proceso

Las nuevas formas de criminalidad han convertido al agente encubierto informático en una pieza fundamental en la investigación penal. Éste es un eslabón de gran importancia en dicha investigación pues sirve para engarzar las investigaciones previas en las que aparecen los indicios delictivos con otras diligencias de investigación, previa determinación del objeto de la investigación; así, la actuación del agente encubierto permitirá no solo corroborar las sospechas de la comisión del delito sino que por medio de su interacción con los sujetos investigados permitirá extender el elemento subjetivo del proceso penal a otros sujetos que inicialmente no eran sospechosos, por lo que se revela como un elemento de investigación imprescindible cuando se trata de delitos cometidos a través de las nuevas tecnologías en los que intervengan una colectividad de sujetos investigados o en el caso de organizaciones criminales.[[2]](#footnote-3)

1. La menor afección de derechos fundamentales de los investigados.

Del mismo modo, no debemos de olvidar que se trata de una medida de investigación menos intrusiva que la mayoría de las diligencias de investigación tecnológicas y, en consecuencia, atendiendo a los principios rectores de las diligencias de investigación tecnológicas regulados en el artículo 588 *bis* de la LECRIM deberá adoptarse con preferencia a otras medidas de investigación como podrían ser el rastreo de equipos de forma remota prevista en el artículo 588 *septies* de la LECRIM o la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos del 588 *quater* también de la LECRIM; medidas éstas que, resultarían más gravosas para el derecho a la intimidad o al secreto de las comunicaciones de los sujetos investigados que la intervención del agente encubierto y, en consecuencia, no podrían acordarse si es adecuada una actuación del agente encubierto informático, so pena de que puedan cuestionarse el auto que las acuerda por contravenir a los principios de necesidad y sobre todo el de excepcionalidad.

Una vez llevada a cabo la actuación del agente encubierto y delimitados los ámbitos objetivo y subjetivo del objeto del proceso penal, sería el momento de adoptar otro tipo de medidas de investigación o, en su caso, proceder a desmantelar la organización criminal, actividad para la cual el agente encubierto ha sido clave al determinar los sujetos que la integran; de este modo, en delitos tan graves como la pederastia, o en aquellos cometidos por organizaciones criminales o de terrorismo, la actuación del agente encubierto informático en los canales cerrados permite determinar a los integrantes de la organización sin ponerlos en alerta para que puedan ser detenidos.

Pese a la enorme relevancia que puede desempeñar el agente encubierto informático en la lucha contra el cibercrimen, lo cierto es que, tal y como vamos a poder analizar en los apartados siguientes, su regulación por el Legislador ha dejado algunas cuestiones fundamentales en el aire.

# La figura del agente encubierto informático.

El agente encubierto informático, como tendremos ocasión de examinar, no es sino una evolución del agente encubierto adaptado a las necesidades de lucha contra el cibercrimen; por dicho motivo, vamos a examinar esta evolución desde la aparición del agente encubierto hasta la aparición del agente encubierto informático con su incorporación al artículo 282 bis de la LECRIM en el año 2015.

Como la realidad suele siempre ir por delante de la norma, el agente encubierto, antes de ser previsto en nuestra LECRIM, venía usándose sin cobertura legal y su empleo fue avalado por la jurisprudencia de la Sala Segunda del Tribunal Supremo. De este modo, el Alto Tribunal señalaba que el empleo de funcionarios de policía bajo una identidad supuesta no era sino una forma de actuación de la policía judicial en cumplimiento de sus funciones investigadoras que nuestro ordenamiento le impone a tenor de lo dispuesto en el artículo 126 de la Constitución Española.[[3]](#footnote-4)

El agente encubierto ha sido definido por el Tribunal Supremo en su sentencia de 13 de marzo de 2019, con cita de otra sentencia de 29 de diciembre de 2010, como un funcionario de policía que actúa en la clandestinidad con identidad supuesta y con la finalidad de reprimir o prevenir el delito.

# Regulación del agente encubierto informático

En el año 1999 la LECRIM introducía el artículo 282 bis añadido por el artículo 2 de la Ley Orgánica 5/1999 que preveía la posibilidad de autorizar a funcionarios de la policía judicial para actuar bajo identidad supuesta autorizados por el Juez o por el Ministerio Fiscal, aunque circunscritos a supuestos de criminalidad organizada.

Este precepto, antes de introducir el agente encubierto informático fue objeto de dos reformas, en los años 2003 y 2010 en las que lo único que hizo el legislador fue expandir aquellos delitos que consideraba incardinados en el ámbito de la delincuencia organizada.

Finalmente, en la reforma del año 2015 se incorpora al artículo 282 bis de la LECRIM el apartado 6, el cual 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 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.

De esta forma, el Legislador crea una figura especial para llevar a cabo una actividad investigadora singular dentro de los denominados canales cerrados de comunicación y que, del mismo modo que el agente encubierto puede llevar a cabo la adquisición o el transporte de los instrumentos del delito, el agente encubierto informático puede transmitir por estos canales cerrados archivos informáticos ilícitos.

Podemos decir que el agente encubierto informático es un agente encubierto el cual, como éste último, actúa con identidad supuesta y cuya principales diferencias son dos: en primer lugar, el agente informático no interactuará, con carácter general físicamente con los investigados al contrario que el agente encubierto; en segundo lugar, hay importantes diferencias en la interacción existente en relación con los instrumentos del delito, pues el agente encubierto informático va un paso más allá que el agente encubierto que solo recibe instrumentos del delito de los investigados bien sea mediante su compra o su transporte mientras que el agente encubierto informático puede intercambiar o enviar archivos ilícitos. Este tipo de interacción activa del agente encubierto informático hacia el investigado, que como veremos se encuentra estrechamente vinculada con la provocación de delito, ha podido ser determinante para que el Legislador haya previsto que, a diferencia del agente encubierto que puede ser habilitado por el Ministerio Fiscal, en agente encubierto informático solo pueda ser habilitado por un órgano jurisdiccional.

Otra especialidad del agente encubierto informático es su ámbito de actuación pues el mismo es más amplio que el del agente encubierto, así, se podrá acordar esta medida de investigación, además de en los supuestos de criminalidad organizada en los que se puede acordar el agente encubierto, en delitos de terrorismo al margen de una organización criminal y en todos los delitos dolosos cuya pena tenga un límite máximo de, al menos 3 años de privación de libertad o que se trate de delitos cometidos a través de medios informáticos.

Sin lugar a dudas, la ampliación de su ámbito de aplicación es una buena muestra de lo idóneo que resulta el agente encubierto informático para la lucha y represión de la ciberdelincuencia. Ahora bien, dada la relevancia que esta figura ostenta en la lucha contra el cibercrimen entendemos que el Legislador ha descuidado determinados aspectos en su regulación legal los cuales traeremos a colación a medida que examinemos la actuación del agente encubierto informático.

# Investigaciones preventivas y agente encubierto informático: una estrecha relación sin caer en la investigación prospectiva.

Al ser el agente encubierto informático un agente de policía es necesario discernir entre la actuación policial que deben de llevar a cabo las fuerzas y cuerpos de seguridad para la prevención del delito de aquella actuación investigadora realizada como policía judicial. Esta dificultad es mayor en el supuesto del agente informático pues en la red, lo normal es actuar, no bajo una identidad falsa o supuesta, sino que se actúa con un nombre de usuario que, en definitiva, oculta la condición de agente de la autoridad.

La prohibición de investigaciones prospectivas entra en juego cuando, de la adopción de una determinada diligencia de investigación se pueden vulnerar derechos fundamentales del investigado en cuyo caso, se requiere adoptar una decisión motivada basada en indicios objetivos de criminalidad y no en meras sospechas tal y como al respecto tiene declarado el Tribunal Constitucional: SSTTC 184/2003 de 23 de octubre y 261/2005 de 24 de octubre.

Por lo expuesto, en la medida de que un funcionario de policía, sin ser habilitado como agente encubierto informático actúe en la red, en canales de comunicación abiertos, no hay colisión alguna con derechos fundamentales y cumple con la finalidad constitucional de prevenir el delito. Ahora bien, en el momento que deba de actuar en canales cerrados de comunicación, al tratarse de un medio de comunicación restringido y actuar con engaño para tener acceso a éstos ya debe de contar con la autorización judicial, la cual, deberá contar con indicios suficientes de criminalidad para justificar la adopción de la intervención del agente encubierto informático.

De hecho, esa actuación previa, que sí será prospectiva pero que no afecta a derechos fundamentales, será necesaria: precisamente para encontrar los indicios racionales de criminalidad que permitan adoptar una intervención del agente encubierto informático. Así lo entiende el Tribunal Supremo cuando se hace eco de esta problemática y señala en su sentencia de 26 de noviembre de 2018 al respecto que carecería de sentido, con el fin de sostener la validez de la diligencia de prueba, la exigencia de que la autorización del agente encubierto se produzca a ciegas, con exclusión de cualquier contacto previo ente la persona que va a infiltrarse en la organización y quienes aparecen como sospechosos de una red delictiva.

La necesidad de averiguar indicios racionales de criminalidad por medio de la función preventiva de los agentes actuando en la red, no solo es válida sino que es necesaria para acordar posteriormente la diligencia de investigación y así lo señala el Tribunal Supremo cuando dictamina 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 se sustente en elementos de juicio dotados de suficiente base empírica para dotar de racionalidad a la medida, tiene algo de contradictorio.[[4]](#footnote-5)

# Necesidad de habilitación judicial mediante resolución motivada.

La actuación del agente policial como agente encubierto informático requiere una autorización judicial que debe de ser motivada tal y como ya hemos apuntado al ver los problemas que se derivaban de esa doble condición de policía y agente encubierto informático.

En relación con la forma de la antedicha autorización judicial, aunque el apartado 6 del artículo 282 bis no se refiera a ello de forma expresa, entendemos que habrá de acordarse mediante auto motivado, *ex* artículo 141 de la LECRIM, en la medida de que va a afectar a un derecho fundamental, como sería el secreto de las comunicaciones, dado que el agente encubierto informático formará parte de un canal cerrado de comunicaciones accediendo a éste último por medio de una identidad supuesta a través del engaño.

Hubiera sido conveniente que, en el apartado 6 del artículo 282 bis de la LECRIM se hubiera hecho una alusión expresa a la necesidad de razonar la decisión de forma similar a lo dispuesto en el apartado 1 del mencionado precepto.

La siguiente cuestión que surge en relación con la autorización judicial es el momento en el que debe producirse ésta. En este sentido entendemos que, en primer lugar y a salvo de cualquier duda, para compartir archivos ilícitos, se requiere contar con la habilitación judicial. Más dudas pueden surgir en relación con la actuación del agente encubierto informático en los denominados canales cerrados de comunicación.

A nuestro modo de ver, el agente encubierto informático requiere, tal y como ya hemos expuesto anteriormente, una autorización judicial para incorporarse a un canal de comunicaciones cerrado mediante su identidad falsa pues está accediendo a comunicaciones que vendrían protegidas por el secreto de las comunicaciones.

Esta posición es la mantenida por la doctrina del Tribunal Supremo cuando señala que la autorización es necesaria para el acceso a un canal cerrado con una identidad falsa tal y como argumenta en la citada sentencia de 26 de noviembre de 2018. En el citado pronunciamiento, entendemos que el Tribunal Supremo incurre en un error al sostener que en el supuesto enjuiciado no se trataba de un canal cerrado de comunicaciones toda vez que se le facilitó la clave del correo electrónico conociendo su verdadera identidad como agente de la Guardia Civil.

En nuestra opinión, que se entregue la clave no influye sobre la naturaleza cerrada o no del canal de comunicación, que se conozca la verdadera identidad afectaría, en todo caso, a la existencia de engaño y, en definitiva, al consentimiento por lo que, de no mediar autorización judicial, el acceso, la prueba obtenida derivada de éste serían válidos por la invitación al canal cerrado consciente y voluntaria dado que no existe vulneración al secreto de las comunicaciones cuando éstas se revelan de forma voluntaria a la persona que recibe la comunicación.

Hecha la anterior matización, hemos de concluir en el sentido de que para que las actuaciones de investigación que realice el agente encubierto informático sean válidas y no vulneren el derecho al secreto de las comunicaciones, la autorización para incorporarse al canal cerrado ha de ser previa a su entrada en el mismo tal y como señala el propio Tribunal Supremo en la doctrina a la que hemos aludido si bien, hubiera sido adecuado incluir esta previsión en el apartado 6 del artículo 282 bis de la LECRIM.

Al hilo de lo anterior surge la duda de qué ha de entenderse por canal cerrado de comunicación. En este sentido el Tribunal Constitucional nos da un concepto de canal abierto de comunicaciones en la STC 241/2012, de 17 de diciembre, FJ 7, señalando por tal, aquel canal del que no puede predicarse su confidencialidad. En sentido contrario por canal cerrado de comunicaciones ha de entenderse aquel en el que existe una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas tal y como señala al respecto la STC 170/2013 de 13 de octubre.

En consecuencia, podemos concluir en el sentido de que en todos aquellos casos en los que la comunicación requiera una previa invitación para poder incorporarse al canal de comunicaciones, por no ser un medio abierto a cualquiera que desee incorporarse, ha de considerarse como un canal cerrado. Es más, en la lógica criminal, el medio empleado para las comunicaciones será uno que permita mantener ese carácter confidencial por razones obvias y, en consecuencia, deberá considerarse como un canal cerrado de comunicaciones atendiendo a la doctrina del Tribunal Constitucional antes expuesta.

# La interacción del agente encubierto con los investigados y el delito provocado.

En el momento en el que el agente encubierto informático entra en contacto con los sospechosos o los investigados, ya sea en su condición de agente de la policía en sus labores de prevención o como agente encubierto informático en el marco de un proceso penal existe una delgada línea que separa el ganarse la confianza de los investigados y la provocación para delinquir.

En la actuación del agente encubierto estos pueden adquirir o transportar objetos ilícitos que implican una colaboración, pero en lo esencial se trata de una conducta pasiva, pero en el caso concreto del agente encubierto informático el hecho de remitir archivos ilícitos supone una conducta más activa lo que a la hora de examinar si ha existido una provocación al delito supone una dificultad añadida.

Esta cuestión se ilustra perfectamente si tomamos como ejemplo una investigación de pederastas en la que ante las sospechas fundadas de que hay un grupo cerrado de usuarios de una red social comparten este tipo de archivos el agente encubierto informático envía archivos ilícitos a uno de los sospechosos y este difunde estas imágenes en el grupo. ¿Es un delito provocado fruto de la actuación del agente encubierto?

Se trata ésta de una cuestión que el Tribunal Supremo, ante la falta de regulación en la LECRIM ha delimitado de forma minuciosa por medio de su jurisprudencia. La citada sentencia de 26 de noviembre de 2018 recoge la doctrina del alto tribunal al respecto y señala lo siguiente:

1. - Existencia de ánimo delictivo propio en los autores.

Se rechaza la existencia del delito provocado al constatar que existió un animus delictivo propio ([Sentencia del Tribunal Supremo de 15 de noviembre de 1989)](http://vlex.com/search?buscable_id=102&buscable_type=Fuente&content_type=2&date=1989-11-15..1989-11-15&filters_order=source&jurisdiction=ES&source=102&tipo_resolucion_1=SEN).

1. - La actividad policial es meramente investigadora.

No hay delito provocado cuando la actividad policial tiene un *animus* tendencial dirigido a realizar una investigación de la actividad de las personas que son sometidas a investigación, y se llevan a cabo operaciones en base a las conversaciones con los implicados que son los que tienen el *animus* inicial delictivo

1. - La conducta del agente es consecuencial a la conducta de los investigados.

No es el agente encubierto el que lleva a cabo las iniciales conversaciones para la operación a desplegar, sino al revés. Que este acepte no quiere decir que sea un delito provocado, sino que éste recibe la información de los investigados y actúa en su calidad de agente encubierto, facilitando la operación a los superiores y fiscalía para el resultado de la operación y la detención. Según los hechos probados se evidencia que "el propósito criminal" ya existía en la mente de los investigados. El agente encubierto lo que actúa es para recibir la información y facilitar la detención, pero no provoca la comisión del delito.

1. - No debe confundirse la investigación del agente encubierto con tomar la iniciativa el autor de una intención delictiva preexistente.

Hay que distinguir entre el delito provocado y la forma de averiguación de un verdadero delito, supuesto en el que el hecho delictivo ya existe y viene determinado por la actuación espontánea del autor, que quiere realizarlo sin estar previamente estimulado por un agente provocador.

1. - Es delito provocado "incitar" a cometerlo con actos manifiestos y claros.

La provocación existe desde el momento en que se incita a estas personas. La Sentencia de esta Sala del Tribunal Supremo 690/2010, de 1 de julio señala que "en el delito provocado resulta ante todo imprescindible el hecho de la inexistencia previa de cualquier actividad delictiva en trance de comisión del concreto delito de que se trate, de modo que si la ejecución del mismo da comienzo sólo a partir de la intervención del funcionario o agente provocador, pudiendo llegar a afirmarse con seguridad que de no haberse producido tal intervención provocativa el delito no se hubiera llegado a cometer, al menos en las circunstancias concretas en las que el mismo se produjo, sí que deviene procedente la calificación, como "delito provocado", de esa conducta ilícita y, por consiguiente, con fundamento en lo inadmisible de dicha provocación por parte de las Autoridades entendida como contribución eficaz y determinante a la comisión de un delito, la procedencia de su carácter impune.

1. - La labor del agente infiltrado no pretende la comisión del delito.

El agente se limita a comprobar la actuación del sujeto, recogiendo pruebas de delitos ya cometidos o que se están cometiendo, como apuntan las Sentencias de esta Sala del Tribunal Supremo de 13 de junio de 2003 y 5 de octubre de 2004, e incluso a realizar algunas actividades de colaboración con el investigado, como añade la sentencia de esta sala de 12 de junio de 2002, que previamente habrá esperado o buscado terceros para la co-ejecución o agotamiento del delito, habiéndose ofrecido el agente infiltrado, adoptando para ello una apariencia de persona normal o simulando ser delincuente, como recoge la sentencia de esta Sala de septiembre de 1993.

1. - El dolo en el autor o autores ya existe antes de la designación del agente encubierto.

El delito arranca de la determinación del sujeto activo, libre, voluntaria y anterior a la intervención del agente policial ([SSTS 5 de octubre de 2004](http://vlex.com/search?buscable_id=102&buscable_type=Fuente&content_type=2&date=2004-10-05..2004-10-05&filters_order=source&jurisdiction=ES&source=102&tipo_resolucion_1=SEN) y [13 de noviembre de 2006)](https://app.vlex.com/vid/25669628), desarrollándose conforme a aquella ideación sin que el agente pueda crear el dolo en los autores, puesto que éstos ya están obrando dolosamente ([STS 23 de junio de 1999)](https://app.vlex.com/vid/17716567).

1. – Los autores actúan libremente.

La actuación policial será lícita mientras permita la evolución libre de la voluntad del sujeto y no suponga una inducción a cometer el delito.

Recapitulando la anterior doctrina del Tribunal Supremo, y aplicándola al ejemplo del canal cerrado de pederastas, si éste estaba formado por pederastas, pero no habían compartido ningún archivo ilícito y comienzan a compartirlos una vez que les llega el material del agente encubierto informático se trataría de un delito provocado y se trataría de una prueba nula. Por el contrario, si el agente se incorpora, previa remisión de archivos ilícitos, pero cuando ya se habían compartido por los miembros del grupo este tipo de archivos con anterioridad es evidente que la prueba será válida.

# La necesaria incorporación de las actas del agente encubierto al proceso y los problemas derivados del momento preclusivo para su aportación.

Una vez obtenida la prueba por el agente encubierto y documentada ésta en las actas nos encontramos con dos problemas: el primero de ellos tiene que ver con el acceso de las partes a estas actuaciones pues, a diferencia de lo que acontece en la regulación de las diligencias de investigación tecnológicas, las cuales son reservadas *ex lege* por disposición del artículo 588 bis letra d de la LECRIM, el artículo 282 bis apartado 6 no dispone nada al respecto.

En este sentido, si como postulamos nosotros, el agente encubierto informático es una especialidad del agente encubierto, le sería de aplicación el párrafo segundo del aparatado 1 del artículo 588 bis de la LECRIM el cual dispone que la resolución por la que se acuerde deberá consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto. La resolución será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad. Sin embargo, no aclara este precepto qué pasa con las actas en las que el agente documente sus actuaciones, ¿Son reservadas también? Indica la antedicha norma en su párrafo tercero que la información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente.

De una primera lectura podemos entender que la información, es decir las actas, se pondrán en conocimiento del juez a la mayor brevedad y añade el precepto que la citada información deberá de ser igualmente aportada al proceso, sin especificar el Legislador el momento en el que la misma deba de ser aportada.

De la parca regulación podemos deducir que hay dos momentos distintos en el tiempo: uno breve y otro indeterminado. De ahí que podamos concluir que la información que obtenga el agente encubierto debe facilitarse regularmente y a la mayor brevedad al juez, y que después debe de aportarse ese conjunto de información de forma completa al proceso, lo que parece comportar que sea en un único acto y, en consecuencia, en un momento distinto, sin determinar la norma de forma expresa cuándo.

La segunda cuestión que deriva de la regulación que estamos examinando es que si la información no es aportada al proceso, las partes la desconocen y ello a pesar de que no se trate de información reservada de forma expresa por la norma, pues del tenor literal de ésta, la única información que tiene carácter reservado es la resolución por la que se acuerde el agente encubierto en la que queda recogida su verdadera identificación.

Esta no es una cuestión baladí dado que el hecho de que las defensas desconozcan elementos incriminatorios relevantes es un obstáculo insalvable para el ejercicio de su derecho de defensa. En este sentido entendemos que, ante la falta absoluta de regulación legal, debería aplicarse el límite máximo para el levantamiento del secreto lo dispuesto en el artículo 302 de la LECRIM y ponerse estas actas a disposición de las partes, diez días antes de la conclusión del sumario. Sin embargo, el Tribunal Supremo, en su reciente sentencia de 27 de febrero de 2019 ha avalado que las actas se incorporen en el acto de la vista sin que ello afecte al derecho a la defensa cuando los elementos incriminatorios de las actas del agente encubierto hayan podido ser conocidos previamente por las defensas a través de las resoluciones procesales.

Es decir, el Alto Tribunal entiende que si el contenido incriminatorio ha sido recogido en resoluciones como el auto de procesamiento o en los autos relativos a la situación personal del investigado, el hecho de que se aporten las actas en su integridad en el acto del juicio no supone la introducción de elementos sorpresivos que menoscaben el derecho a la defensa.

Llegados a este punto y aunque podamos compartir la tesis del Tribunal Supremo de que no hay menoscabo del derecho de defensa, nos parece conveniente que el Legislador regule esta cuestión y establezca un momento exacto a partir del cual las actas del agente encubierto deban ser conocidas por las partes para evitar hacer exámenes supuesto a supuesto para ver si en ese proceso concreto las resoluciones procesales contenían la totalidad del contenido incriminatorio de las actas del agente encubierto pues esto se presta a que cualquier pequeña omisión genere una indefensión que dé lugar a una nulidad del proceso penal, cuestión ésta que es fácilmente evitable fijando un momento procesal para que las defensas conozcan su contenido antes de las sesiones del juicio oral. Este momento podría ser perfectamente el plazo máximo en el que ha de levantarse el secreto de sumario, es decir, 10 días antes de que se dicte el auto de conclusión del sumario.

#  La necesaria ratificación en el acto del juicio del agente encubierto.

La segunda de las cuestiones que se plantean en relación con la incorporación de la prueba del agente encubierto informático es la necesidad de su comparecencia en el juicio para ratificar el contenido documentado en las actas. A fin de que quede garantizado el principio de contradicción es necesario que el agente encubierto informático comparezca en el acto del juicio oral y, además de ratificar el contenido de sus actas, responda a las preguntas de ambas partes.

El Tribunal Supremo se muestra inflexible en este punto y no permite que el contenido de las actas pueda ratificarse mediante declaraciones de referencia tal y como de forma meridianamente clara recoge en su sentencia de 27 de febrero de 2019.

Obviamente, el agente encubierto podría declarar ocultando su identidad para preservar su anonimato en futuras operaciones, sin embargo, en el supuesto concreto del agente encubierto informático, en principio no sería necesario dado que su alias o identidad ficticia ya ha quedado comprometida y lo importante no es preservar en secreto sus características físicas como sucede con el agente encubierto, por lo que, a priori no sería necesario ocultar su identidad en el acto del juicio.

# La prueba obtenida por el agente encubierto como base de una condena penal.

Como acabamos de ver la prueba obtenida por el agente encubierto será una prueba válida y no vulnerará los derechos fundamentales en los términos del artículo 11 de la LOPJ cuando se den los siguientes requisitos:

* Existencia de unos indicios previos de la posible comisión de un delito.
* Adopción de la medida de investigación del agente encubierto informático mediante auto motivado antes de que éste se introduzca en un canal cerrado de comunicaciones mediante una identidad falsa.
* El agente encubierto no provoque el delito.

Además de los requisitos relativos a la validez de la prueba, la condena penal fundada en dicha prueba requiere la existencia de un proceso con todas las garantías lo que, en relación con la prueba exige lo siguiente:

* Que las defensas hayan conocido el contenido incriminatorio de las actas del agente encubierto informático antes del juicio, pues de otra manera, el derecho a la defensa no quedaría garantizado pues existiría indefensión.
* El agente encubierto informático, en el acto del juicio deberá ratificar el contenido de las actas y someterse al interrogatorio de las partes para que quede garantizado el principio de contradicción.

Cumplidas las anteriores exigencias, la prueba del agente encubierto informático será una prueba válida practicada en un proceso con plenas garantías y, en consecuencia, podrá servir como fundamento de la condena penal.

En caso de que no concurran los tres primeros requisitos, se tratará de una prueba nula por vulnerar derechos fundamentales *ex* artículo 11 de la LOPJ y, en consecuencia, no podrá considerarse para la condena, con independencia de que se hayan cumplido los requisitos procedimentales relativos a su incorporación al proceso y práctica en el acto del juicio.

Por el contrario, si el vicio se produjese en su incorporación al proceso o en su práctica, ello conllevaría una nulidad de actuaciones, pero nada impediría que, subsanado la infracción procesal, dicha prueba sirva para fundamentar la condena.

# Luces y sombras del agente encubierto informático.

Las principales aportaciones que hace esta diligencia de investigación a nuestro proceso penal es que se trata de una medida idónea para las fases de la investigación más incipientes en las que los elementos del objeto del proceso, principalmente el subjetivo, aunque también el objetivo, no ha sido aún determinados y que, tal y como ya ha quedado expuesto anteriormente, se trata de una diligencia de investigación cuya afección a derechos fundamentales de los investigados es mucho menor que otras diligencias de investigación tecnológica por lo que, previamente a adoptar otras diligencias que afecten en mayor grado a los derechos fundamentales de los investigados, se puede emplear el agente encubierto informático para determinar los elementos del objeto y la gravedad de los hechos.

Otra importante ventaja de esta figura es que permite acceder a organizaciones criminales cuya actividad ilícita se desarrolla en los canales cerrados de comunicación que de otra forma serían prácticamente imposible de investigar.

En el activo de esta figura podemos situar el hecho de que los presupuestos procesales para la adopción de esta diligencia de investigación, al comportar un menor grado de afección de derechos fundamentales, son menos estrictos que los previstos para la adopción de otras medidas de investigación tecnológicas y se puede emplear en un mayor número de supuestos penales, lo que la convierte en un medio mucho más accesible para la investigación del cibercrimen y una herramienta más versátil. De este modo, bastará con que se trate de la investigación del alguno de los delitos previstos en el apartado 6 del artículo 282 bis de la LECRIM y que existan indicios de su perpetración para que el juez encargado de la investigación pueda acordarlas.

En relación con las sombras existentes en torno al agente encubierto informático, el principal problema es que el Legislador no ha prestado a esta figura la debida atención y en gran medida se trata de una figura que, aunque prevista en la LECRIM, los aspectos más relevantes de su regulación, tal y como hemos tenido oportunidad de examinar en el presente trabajo, no están regulados en la LECRIM sino que los ha determinado el Tribunal Supremo por medio de su jurisprudencia.

En este sentido podemos afirmar que el Legislador debería regular el momento procesal oportuno a partir del cual los agentes deben de solicitar esta autorización al juez y despejar dudas tan relevantes como si el agente encubierto puede, sin usar una información falsa relativa a su identidad y en el ámbito de la prevención del delito, incorporarse a un canal cerrado por medio de un alias o nombre de usuario

También sería muy conveniente que se estableciera una regulación atinente al secreto de esta diligencia pues a nadie se le puede escapar que el buen fin de este tipo de diligencias de investigación conllevan la necesidad de que las partes que están siendo investigadas desconozcan la existencia tanto del propio agente encubierto informático, circunstancia ésta que sí aparece regulada en el apartado 1 del artículo 282 bis, pero también del resultado de sus investigaciones documentado por medio de actas.

Nos parece que esta regulación debería establecer un momento preclusivo a partir del cual, las actas del agente encubierto informático deben de quedar disponibles para las partes sin perjuicio de que parte de su contenido incriminatorio sea recogido en resoluciones procesales, pues de esta forma, se evita que, si parte del contenido incriminatorio no ha quedado recogido en las resoluciones procesales y las partes acusadas lo desconocen hasta el momento del juicio, pueda cuestionarse la existencia de indefensión.

En cualquier caso, la parca regulación relativa a la aportación al proceso de las actas puede colmarse mediante la aplicación supletoria del secreto de sumario que podría aplicarse solo en lo relativo a las investigaciones que realice el agente encubierto, aunque en este último caso las actas deberían aportarse íntegramente en los 10 días anteriores a la conclusión de la instrucción y no en un momento posterior como permite la doctrina del Supremo.

# Conclusiones

La evolución del cibercrimen y las especiales características de la figura del agente encubierto informático relativas a su naturaleza, su funcionamiento y el escaso grado de afección que puede ocasionar sobre los derechos fundamentales de los investigados hacen que se trate de una diligencia de investigación que está llamada a ser imprescindible en la lucha contra éste, sobre todo cuando se trate de organizaciones integradas por varios sujetos.

El agente encubierto informático es una especialidad del agente encubierto y, en consecuencia, se le aplica tanto la regulación legal como jurisprudencial de este último en todo aquello no previsto en su regulación.

La validez de la prueba obtenida por el agente encubierto informático requiere que la adopción de la diligencia se haya adoptado mediante auto motivado, previa constatación de unos indicios objetivos de criminalidad que determinen la ausencia de una investigación prospectiva en la adopción de la medida de investigación y que en la interacción del agente encubierto informático con los investigados no tenga lugar una provocación al delito que dé lugar a la existencia de un delito provocado por el agente encubierto informático.

En cuanto a la incorporación de la prueba válidamente obtenida al proceso penal, ésta se documentará en actas que deben de ser trasladadas, a medida que se produce, al juez que adopta la medida de investigación y, una vez concluida la investigación, ser incorporadas en su totalidad al proceso para el conocimiento de las defensas aunque la doctrina jurisprudencial del Supremo permite que este momento se dilate hasta el juicio oral siempre y cuando su contenido incriminatorio haya sido conocido por las defensas a través de su transcripción en las resoluciones procesales que se han producido.

En cuanto a la práctica de la prueba, el Supremo tiene declarado que el agente encubierto informático habrá de comparecer en el acto del juicio y ratificar el contenido de las actas sin cuya comparecencia no podrá ser considerada por el juez o tribunal sentenciador.

Pese a la magnífica labor de la jurisprudencia del Tribunal Supremo en relación con esta figura a la que otorgó carta de naturaleza antes incluso que el propio Legislador y aunque en la actualidad dicho Alto Tribunal siga colmando las importantes lagunas que su regulación presente en relación al momento en que debe de ser acordada su habilitación judicial o en relación a su carácter reservado y el levantamiento de éste, esta deficiente regulación supone una mayor inseguridad jurídica y la necesidad de analizar cada proceso a la hora de determinar si el derecho de defensa ha quedado garantizado por lo que sería más que conveniente que el Legislador, en posteriores reformas, atienda un poco más a esta figura y perfile estas cuestiones teniendo en cuenta la doctrina del Supremo como hizo al regular las diligencias de investigación tecnológicas.

BIBLIOGRAFÍA

BUENO DE MATA, F., “Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿deberían ampliarse las actuales funciones del agente encubierto en internet? en *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito* Coordina PÉREZ GIL, J., La Ley, 2012, págs. 311 a 330.

RIZO GÓMEZ, B., “La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en 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” en AAVV *Justicia Penal y nuevas formas de delincuencia,* Dirige ASENCIO MELLADO, J.M., Valencia, 2017.

SÁNCHEZ GÓMEZ, R., “El agente encubierto informático” en *LA LEY PENAL,* número 118, 2016.

VALIÑO CES, A., “Una lectura crítica en relación al agente encubierto informático tras la Ley Orgánica 13/2015” en *DIARIO LA LEY*, número 8731, 2016.

VILLAR FUENTES, I., “Reflexiones sobre el agente encubierto informático” en *El proceso penal: Cuestiones fundamentales,* coordina FUENTES SORIANO, O., Valencia, 2016.

1. Datos estadísticos publicados por el Ministerio del Interior en el siguiente sitio web: <https://www.google.com/search?ei=jIb3XMS2LpHylwSF_JPoCw&q=estadisticas+delitos+informaticos+espa%C3%B1a&oq=estadisticas+delitos+info&gs_l=psy-ab.1.0.0l4j0i22i30l6.4613.6985..8406...0.0..0.117.1069.1j9......0....1..gws-wiz.......0i71j0i67.BhwvCWIIT7g> (Última consulta 5 de junio de 2019) [↑](#footnote-ref-2)
2. Así lo indica BUENO DE MATA cuando señalaba que imputar determinados delitos a sus presuntos autores resulta una tarea difícil, más aún si cabe en el plano virtual, donde el anonimato que ofrece la red complica esta tarea aún más si cabe. BUENO DE MATA, F., “Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿deberían ampliarse las actuales funciones del agente encubierto en internet? en *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito* Coordina PÉREZ GIL, J., La Ley, 2012, págs. 311 a 330. [↑](#footnote-ref-3)
3. Sentencia del Tribunal Supremo de 5 de junio de 1999. [↑](#footnote-ref-4)
4. STS de 26 de noviembre de 2018. [↑](#footnote-ref-5)