Facultad de Derecho
Universidad Zaragoza

Universidad Zaragoza
1542

TRABAJO FIN DE GRADO

Derecho Procesal Penal

EL AGENTE ENCUBIERTO INFORMÁTICO

Alumno: ALEJANDRO CLUSA LÓPEZ (625549)

Tutora: Dª Mª ROSA GUTIÉRREZ SANZ

Facultad de Derecho, 2018/2019

Facultad de Derecho
Universidad Zaragoza

ÍNDICE

I.- ABREVIATURAS

AEI: Agente Encubierto Informático
LECrim: Ley de Enjuiciamiento Criminal
CE: Constitución Española
LO: Ley Orgánica
LOPJ: Ley Orgánica del Poder Judicial
STC: Sentencia del Tribunal Constitucional
STS: Sentencia del Tribunal Supremo
STEDH: Sentencia del Tribunal Europeo de Derechos Humanos
TEDH: Tribunal Europeo de Derechos Humanos
SAN: Sentencia de la Audiencia Nacional

II.- INTRODUCCIÓN

Razón de la elección del tema:

Con el auge de las nuevas tecnologías, la era virtual que empapa la gran mayoría de actividades cotidianas y una sociedad interconectada, resulta de vital importancia regular todo lo que concierne a ese espacio de interconexiones. De igual modo que cualquier invención siempre ha supuesto un cambio en la forma de vida de cada uno de nosotros, Internet, red global que nos enlaza a todo el mundo, no ha sido menos.

Esa influencia de Internet en nuestra vida diaria ha supuesto un antes y un después. La gran mayoría de gestos y actos que llevamos a cabo con total espontaneidad, en cierta manera, pasan o dependen de la red. El mero hecho de recibir un WhatsApp en el teléfono móvil en nuestro bolsillo, aplicaciones que nos facilitan poder hacer la compra online y un infinito etcétera pasa por esa red global. Internet goza de un elemento que hace que sea muy complicada la detección y persecución de un delito en la red, dadas las posibilidades de entrar como usuario anónimo y por la falta de responsabilidad con la que a veces se accede a la red, sin ser conscientes de todo lo que puede acarrear el omitir unas medidas de seguridad mínimas para navegar seguros.

La dependencia directa o indirecta de Internet conlleva también peligros a los que hacer frente. Esa interconectividad, esa facilidad para acceder a un inmenso mundo virtual desde edades muy tempranas, hace que en muchas ocasiones no seamos conscientes de la peligrosidad a la que podemos estar enfrentándonos. Como en otras muchas facetas de la vida diaria, la realidad va cinco pasos por delante de la regulación, de hecho, la regulación se va desarrollando conforme se va analizando y detectando como va variando la realidad, que formas de delinquir o defraudar están a la orden del día, etc. Se va dando forma normativa y de regulación una vez que se ha contrastado ese nuevo fenómeno.

Cuestión tratada en el Trabajo Fin de Grado:

Con la figura del agente encubierto informático pasa algo similar a ese fenómeno descrito anteriormente, puesto que la realidad se anticipa a la regulación y ésta va cogiendo forma y contenido a raíz de los resultados detectados previamente.

En consecuencia, el legislador consideró necesario hacer una reforma de la LECrim, haciendo hincapié en ese mundo virtual o también llamado 2.0, tal como recoge el Preámbulo de la propia Ley en su apartado IV, reconociendo que los flujos de información generados por los sistemas de comunicación telemática advierten de las posibilidades que se hallan al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos. Surge así la necesidad de encontrar un equilibrio entren la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros.

En la misma línea, el Preámbulo de la LO 13/2015 se hace eco de que las medidas de investigación tecnológica, caso del agente encubierto informático, deben satisfacer los principios constitucionales de idoneidad, excepcionalidad, necesidad y proporcionalidad, cuya concurrencia debe encontrarse suficientemente justificada en la resolución judicial habilitadora, donde el juez determinará la naturaleza y extensión de la medida en relación con la investigación concreta y con los resultados esperados.

Se pretende con ello que sea el propio juez, ponderando la gravedad del hecho que está siendo objeto de investigación, el que determine el alcance de la injerencia del Estado[1].

No sólo con la LO 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, se pretendió ampliar la anterior lista tasada[2] de delitos bajo los que un Policía Judicial con la correspondiente autorización judicial podía ejercer como agente encubierto, sino que también se incluyó, por ejemplo, que pudieran 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.

Incluso, el juez 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.

Mediante la inclusión, entre otros, de estos dos apartados 6º) y 7º) al artículo 282 bis de la LECrim, que centrarán este Trabajo Fin de Grado, se pretende poner fin a un vacío normativo, así como actualizar las competencias de la concepción clásica del agente encubierto adaptadas a las necesidades que requiere la investigación tecnológica para dotar de medios y seguridad a los procedimientos que se lleven a cabo para perseguir la ciberdelincuencia.

Metodología seguida en el desarrollo del trabajo:

Se parte del artículo 282 bis de la LECrim, concretamente, de los ya enunciados apartados 6º) y 7º), mediante los que se regula el agente encubierto informático. El objetivo de este trabajo será aportar una visión simplificadora a la vez que profunda de esta medida de investigación tecnológica haciendo una distinción con otras figuras de investigación que en ocasiones pueden llevar a equívoco, como es el agente provocador.

[1] Preámbulo LO 13/2015, de 5 de octubre de 2015, de modificaciones de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (BOE 6 de octubre 2015).
[2] Artículo 282 bis. 4 LECrim.

Por un lado, se desarrollarán las diferentes modalidades de actuación del agente encubierto informático, bien por el tipo de canal de comunicación en que desarrolle su actividad o bien por las diferentes competencias que le atribuye la ley y su relación con los derechos fundamentales.

Por otro lado, se hará un análisis de la autorización necesaria por la que un juez de instrucción habilita a la Policía Judicial para actuar como agente encubierto informático. Asimismo, se incidirá en los principios básicos que guían la actuación del agente encubierto informático, así como los diferentes tipos de responsabilidad que éste puede llegar a asumir.

En último lugar, se profundizará en los efectos procesales de la actividad encubierta del agente en lo referente a su declaración y efectos probatorios.

III.- CONCEPTO

El agente encubierto es una figura legal dentro de nuestro ordenamiento jurídico que permite a los miembros de la Policía Judicial participar del entramado organizativo bajo una identidad supuesta para detectar la comisión de delitos e informar sobre sus actividades, con el fin de obtener pruebas inculpatorias y proceder a la detención de sus autores [3] y que se circunscribe, en su inicio, a las investigaciones relacionadas con el tráfico de drogas y otros delitos graves.

En este apartado se analizará en profundidad la figura del agente encubierto informático y se comparará con el agente provocador, una figura proscrita en nuestro ordenamiento que, en ocasiones, puede ser erróneamente identificada con el agente encubierto.

3.1.- EL AGENTE ENCUBIERTO INFORMÁTICO

Se trata de un miembro de las Fuerzas y Cuerpos de Seguridad del Estado que, voluntariamente, y mediando la correspondiente resolución judicial, se infiltra en la Red con el fin de obtener información sobre las prácticas delictivas producidas a través de la misma[4].

[3] Exposición de Motivos, Ley Orgánica 5/1999, de 13 de enero, de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves. (BOE 14 de enero de 1999).

[4] ZARAGOZA TEJADA, J. y BERMÚDEZ GONZÁLEZ J. *Investigación tecnológica y derechos fundamentales*. Cizur Menor (Navarra), 2017.: Aranzadi-Thomson Reuters. p.329.

El agente encubierto informático es una especialidad dentro de los agentes encubiertos, un instrumento de investigación por el que un policía judicial puede actuar bajo una identidad fingida en comunicaciones a través de canales cerrados de comunicación con el fin de esclarecer alguno de los delitos cometidos en el seno de organizaciones criminales así como otros previstos en el artículo 588.ter.a LECrim; pudiendo el agente analizar e intercambiar archivos de contenido ilícito así como obtener imágenes y grabar conversaciones privadas que se mantengan con el investigado[5].

La STS 1140/2010, de 29 de diciembre, define así al agente encubierto:
"*El término undercorver o agente encubierto, se utiliza para designar a los funcionarios de policía que actúan en la clandestinidad, con identidad supuesta y con la finalidad de reprimir o prevenir el delito. Agente encubierto, en nuestro ordenamiento será el policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la Ley y bajo el control del Juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación o estos sean manifiestamente insuficientes, para su descubrimiento y permite recabar información sobre su estructura y modus operandi, así como obtener pruebas sobre la ejecución de hechos delictivos, debiéndose aclarar que es preciso diferenciar esta figura del funcionario policial que de forma esporádica y aislada y ante un acto delictivo concreto oculta su condición policial para descubrir un delito ya cometido"*[6].

En el mismo sentido, la STS 395/2014, de 13 de mayo de 2014, FJ 3º, prevé que el agente encubierto *"ha de tratarse de un miembro de la policía judicial que, por resolución motivada, recibe una especie de autorización para transgredir la norma respecto a alguno de los delitos que se relacionan en el artículo 282 bis, una especie de excusa absolutoria impropiamente recogida en una norma procesal"*[7].

En paralelo, la STS 345/2019, de 7 de febrero, refiere que *" la actuación del agente encubierto con la oportuna autorización judicial es una medida apta y hábil ... reconocida legalmente para la obtención de pruebas con respecto a los hechos que son objeto de*

[5] JURADO FORTES M., "Agente encubierto informático", López de Lemus Abogados. (disponible en https://lopezdelemus.com/agente-encubierto-informatico/ ; última consulta 11/05/2019).
[6] STS 1140/2010, de 29 de diciembre de 2010 (FJ6), (disponible en https://supremo.vlex.es/vid/-252334458; última consulta 30 de abril de 2019).
[7] STS 395/2014, 13 de mayo de 2019 (FJ3), (disponible en https://supremo.vlex.es/vid/-514868514; última consulta 1 de junio de 2019).

investigación, y en donde, al igual que las medidas de limitación de derechos fundamentales se llega un punto en la investigación en donde ya no se puede continuar, precisando la introducción de medidas de investigación, como la del agente encubierto, para acceder a esa información de la que no podría accederse de otra manera; y más en circuitos informáticos de comunicación cerrados que requieren de claves o accesos de amistas entre los partícipes"[8].

La STS 140/2019, de 13 marzo, haciendo referencia a esta especialidad de agente encubierto recoge que *"La reforma de LO 13/2015 ha introducido los apartados 6 y 7 del artículo 282 de la LECrim. El apartado 6 introduce la novedosa figura del agente encubierto informático, tratando el legislador, una vez más, de adaptar el texto legal a la sociedad digitalizada en la que nos encontramos inmersos"*[9].

Como se decía en la sentencia precedente, la figura del agente encubierto informático se creó con 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 incorporando los apartados 6º) y 7º) al artículo 282 bis[10]. Dicha Ley, detalla los supuestos en los que podrá acordarse la intervención del agente encubierto. Esa intervención se podrá producir exclusivamente en una serie de supuestos tasados, y siguiendo un procedimiento considerablemente garantista[11].

[8] STS 345/2019, de 7 de febrero de 2019 (disponible en http://www.poderjudicial.es/search/openCDocument/cac2ec927df2ac2484b8072b28c6b92ae0bfc5e75133822b; última consulta 1 de mayo de 2019).

[9] STS 140/2019, de 13 de marzo de 2019 (disponible en https://supremo.vlex.es/vid/773754989; última consulta 1 de junio de 2019).

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

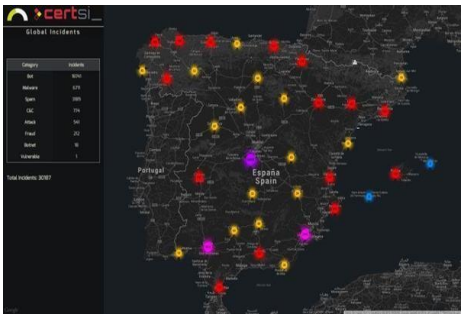
art. 282. bis.7) LECrim. *"En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio".*

[11] Cfr. con MARCHENA GÓMEZ, M., GONZÁLEZ CUELLAR SERRANO, N., *La reforma de la Ley de enjuiciamiento criminal en 2015*. Madrid, 2015.

El ejercicio de la función de agente encubierto informático se encuentra reservado para los integrantes de la Policía Judicial quedando por tanto excluidos el resto de los miembros de las Fuerzas y Cuerpos de Seguridad del Estado.

La infiltración informática policial supone, en muchas ocasiones, el único modo de detección y prevención de la ciberdelincuencia. Hoy en día, la delincuencia tradicional en parte ha quedado relegada ante las nuevas formas entendiendo como tal, los ataques cibernéticos a empresas, fraudes económicos vía internet, acoso en la red, etc.

Para situar la vulnerabilidad a la que actualmente está sometida la sociedad, valga como ejemplo, España, que es el tercer país a escala mundial a quien más afecta la ciberdelincuencia, con 200.000 ciberataques diarios[12].



Goicoechea N., España, tercer país del mundo en ciberataques.

3.2.- DIFERENCIA ENTRE LA FIGURA DEL AEI Y LA DE AGENTE PROVOCADOR

El concepto de "provocación al delito" es incorporado por el artículo 282 bis LECrim recogiendo en su apartado 5º) que *"el agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de esta y no constituyan una provocación al delito".* Este concepto ha tenido que ir concretándose con diferente jurisprudencia.

[12] El mapa incluido en el trabajo se ha extraído de GOICOECHEA. N." España, tercer país del mundo en ciberataques" (disponible en https://cadenaser.com/ser/2014/11/25/ciencia/1416920321_278876.html ; última visita 14 de abril de 2019).

La STS 204/2013, de 14 de marzo, recoge en su Fundamente de Derecho 1º) y siguiendo la postura del Tribunal Europeo de Derecho Humanos (TEDH), que "*se considera que ha tenido lugar una provocación por parte de la policía cuando los agentes implicados -ya sean miembros de las fuerzas de seguridad o personas que actúen según sus instrucciones- no se limitan a investigar actividades delictivas de una manera pasiva, sino que ejercen una influencia tal sobre el sujeto que le incitan a cometer un delito que, sin esa influencia, no hubiera cometido, con el objeto de averiguar el delito, esto es, aportar pruebas y poder iniciar un proceso"* (STEDH en el caso Ramanauskas contra Lituania, de 5 de febrero de 2008).

Esta misma sentencia añade que *"el interés público no podría justificar la utilización de datos obtenidos tras una provocación policial", pues tal forma de operar es susceptible de privar definitivamente al acusado de su derecho a un proceso equitativo"* [13].

A) AGENTE PROVOCADOR

Se entiende como aquel sujeto que incita a la realización de un determinado hecho[14]. Para GIMENO SENDRA[15] es un miembro de las Fuerzas y Cuerpos de Seguridad que, con la finalidad de descubrir un hecho delictivo llega a instigar a propiciar la comisión del delito con las peticiones que le formulen a los imputadores.

En España no se contempla dentro de la regulación positiva y la intervención de un agente provocador en el tráfico jurídico está prohibida a pesar de que la jurisprudencia sí ha aceptado su práctica. En este sentido, ha basado su admisión en la diferencia existente entre la figura y el delito provocado que a continuación se examinará.

[13] STS 204/2013, de 14 de marzo, Sala Segunda de lo Penal (FD1º) (disponible en https://supremo.vlex.es/vid/delito-salud-provocado-429311538; última consulta 19 de abril de 2019).
[14] RUIZ ANTÓN, LF., *El agente provocador en el derecho penal*, Edersa, Madrid, 1982, p.6.
[15] GIMENO SENDRA, V., *Manual Derecho Procesal Penal*, Castillo de Luna Ediciones Jurídicas, Madrid 2018, p. 407.

B) DELITO PROVOCADO

La STS 395/2014, de 13 de mayo, precisa en su 4º) Fundamento de Derecho qué se entiende por delito provocado:

"El delito provocado se integra por una actuación engañosa del agente policial que supone una apariencia de delito, ya que desde el inicio existe un control absoluto por parte de la policía. Supuesto distinto es la actividad del agente tendente a verificar la comprobación del delito. No puede pues confundirse el delito provocado instigado por el agente con el delito comprobado a cuya acreditación tiende la actividad policial.

El delito provocado se integra por tres elementos:

1. *Un elemento subjetivo constituido por una incitación engañosa a delinquir por parte del agente a quien no está decidido a delinquir.*
2. *Un elemento objetivo teleológico consistente en la detención del sujeto provocado que comete el delito inducido.*
3. *Un elemento material que consiste en la inexistencia de riesgo alguno para el bien jurídico protegido, y como consecuencia la atipicidad de tal acción"*[16].

En el 2º) Fundamento de Derecho de la STS 863/2011, se decía que "*el delito provocado, según una consolidada doctrina de esa Sala de Casación, aparece cuando la voluntad de delinquir surge en el sujeto no por su propia y libre decisión, sino como consecuencia de la actividad de otra persona, generalmente un agente o un colaborador de los Cuerpos o Fuerzas de Seguridad , que, guiado por la intención de detener a los sospechosos o de facilitar su detención, provoca a través de su propia y personal actuación engañosa la ejecución de una conducta delictiva que no había sido planeada ni decidida por aquél, y que de otra forma no hubiera realizado, adoptando al propio tiempo las medidas de precaución necesarias para evitar la efectiva lesión o puesta en peligro del bien jurídico protegido"* [17].

[16] STS, Sala Segunda de lo Penal, STS 289/2015 de 28 de septiembre de 2015, (FD 4º) (disponible en https://supremo.vlex.es/vid/586988258, última consulta 20 de abril de 2019).
[17] STS 863/2011, de 21 de julio de 2011, Sala Segunda de lo Penal (FD2º) (disponible en https://supremo.vlex.es/vid/-310932130, última consulta 19 de abril de 2019).

RIFÁ SOLER, JM[18] considera delito provocado el que tan sólo llega a realizarse en virtud de inducción engañosa de un agente de las Fuerzas y Cuerpos de Seguridad que, deseando conocer la propensión al delito de persona o personas sospechosas y para que se lleve a cabo su torcida inclinación, estimula simulando allanar y desembarazar el *iter criminas*.

Consecuencia de lo anterior, es lógica la asignación de la cualidad de agente provocador al que impulsa a otro a cometer un delito para determinar su responsabilidad. La consecuencia de la provocación delictiva para la justicia es el resultado contrario al que se pretendía, es decir, las personas que han sido objeto de inducción quedarán impunes de los hechos acecidos[19].

Hay que tener muy presente que en caso de tratarse de un delito provocado se lesionaría el principio de interdicción de arbitrariedad de los poderes públicos (art. 9.3 CE), así como los derechos a la presunción de inocencia y a la tutela judicial efectiva.

Una vez que se ha analizado el concepto del agente encubierto informático y el apartado correspondiente al agente provocador, se extraen notas comunes de las dos figuras. En ambos casos se trata de un miembro de las Fuerzas y Cuerpos de Seguridad. También se les atribuyen competencias para investigar organizaciones criminales, y, además se les presume de cierto grado de confianza con el investigado.

Sin embargo, a tenor del artículo 282bis 5) LECrim, el agente encubierto informático tiene prohibida la provocación, siendo ésta uno de los límites de su actuación y uno de los motivos por los que el agente encubierto podrá tener responsabilidad criminal. Además, como ya se ha dicho, el agente provocador no se contempla dentro de la regulación positiva por lo que no tiene habilitación legal, al contrario que el agente encubierto que sí está regulado en el artículo 282bis LECrim.

[18] RIFÁ SOLER, JM, "El agente encubierto o infiltrado en la nueva regulación de la Ley de Enjuiciamiento Criminal*", Revista del Poder Judicial, nº55, CGPJ*, 1999. SILVA SÁNCHEZ, JM. "La consideración del comportamiento de la víctima", *Cuadernos del Consejo General del Poder Judicial*.

[19] MONTÓN GARCÍA, M.L., "Agente provocador y agente encubierto: ordenemos conceptos*", La Ley*, nº 4826, 1999, p.2128.

IV.- SUPUESTOS EN QUE SE PERMITE LA ACTIVIDAD ENCUBIERTA

Como más adelante se analizará, la actuación del agente encubierto informático comporta una actividad en muchos casos, limitativa de derechos fundamentales, por ello, sólo será acordada en aquellos casos en que la gravedad del delito así lo aconseje.

La propia LECrim determina que el juez de instrucción podrá autorizar a miembros de la Policía Judicial a utilizar una identidad fingida para actuar bajo la figura del agente encubierto informático e investigar y esclarecer los delitos contemplados en el artículo 282 bis 4) LECrim y también para aquellos delitos cometidos a través de instrumentos informáticos o de cualquier tecnología de la información o servicio de comunicación, regulados en artículo 588 ter a) LECrim.

En definitiva, esta medida tiene cabida en todas aquellas actividades que se puedan considerar como actividades propias de delincuencia organizada, que se encuentran definidas y enumeradas numerus clausus en la propia ley. El requisito de que debe tratarse de delincuencia organizada da lugar a que no se puedan investigar por esos medios muchos delitos que se cometen hoy en día.

De hecho, VILLAR FUENTES[20] afirma que el potencial alcance y daño de la actividad criminal no precisa en ocasiones de delincuencia organizada entendida como la agrupación de tres o más personas, sino que puede ser más dañino y extenso, con la mera utilización de cualquier canal informático.

El requisito de delincuencia organizada puede ser un impedimento para la figura del agente encubierto informático, precisamente, para uno de los principales objetivos de la figura, refiriéndose, concretamente, al acoso de menores, ya que ese tipo de delitos es más propio de delincuencia individualizada[21].

[20] VILLAR FUENTES M.I. "El agente infiltrado y las diligencias de investigación tecnológica." *Archivio penale 2017, nº 2, Dall´Europa* p .15 (disponible en http://www.archiviopenale.it/File/Download?codice=4f03a98a-2ff7-4b47-beaf-f85630bbc39c; última visita 1 de junio de 2019).

[21] 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, pág. 24 y 25; disponible en

Con esta reforma o ampliación de los delitos se consigue poder investigar conductas ilícitas como acoso a menores de edad, el ataque a sistemas informáticos, estafas a través de internet, adoctrinamiento terrorista, ciberacoso, pornografía infantil, extorsión, etc. y que no aparecen enumerados en la lista.

Tal es la importancia de esta figura de investigación tecnológica que el Anteproyecto de Ley Orgánica para un nuevo Proceso Penal planteó también la inclusión de un nuevo apartado al art. 282 bis, referido, igualmente, al tratamiento del agente encubierto informático[22].

Pese a lo recogido en los apartados 6º) y 7º), que introdujo la Ley Orgánica 13/2015, no se tasan los casos en que el agente encubierto informático, en el ejercicio de sus funciones, estaría amparado por su carácter, o por el contrario, estaría incurriendo en un tipo penal. Esto se salvará haciendo una interpretación a la postre del juicio de la legitimidad constitucional de la medida en cuanto haya podido afectar a los derechos fundamentales.

V.- MODALIDADES DE ACTUACIÓN DEL AEI

5.1.- CANALES DE COMUNICACIÓN CERRADOS

En la LO 13/2015 se hace referencia expresa a la actuación del agente encubierto informático dentro de comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer algunos delitos.

La propia Exposición de motivos de la Ley 13/2015 recoge precisamente que sólo requiere autorización judicial la figura del agente encubierto informático para actuar en canales cerrados de comunicación (puesto que en los canales abiertos, por su propia naturaleza, no es necesaria) 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 su investigación. Un canal cerrado es aquel en que es necesaria una identificación previa para acceder.

---

https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/INFORME_CF_MODIFICACIÓN_LECrim_23-01-2015.pdf?idFile=7c2cd525-01bf-4cc0-864a-29dc8ee0dae9; última consulta 5 de mayo de 2019).

[22] VILLAR FUERTES, M.I., "El agente infiltrado y las diligencias…", cit. p.3ss.

A tenor de la jurisprudencia del Tribunal Supremo[23], la utilización del agente encubierto no excluye la posibilidad de que, con carácter previo al uso de esta figura, los agentes de las fuerzas y cuerpos de seguridad del estado puedan realizar una investigación precedente que implique tomar contacto con alguno o algunos de los investigados a fin de reunir elementos indiciarios suficientes que permitan abrir una investigación judicial más definida[24].

La STS 3693/2013, 28 de junio de 2013[25], enmarca la existencia de un contacto previo entre el recurrente y el agente encubierto, "*en una relación derivada de las labores de prevención y captación de información propias de las Fuerzas y Cuerpos de Seguridad del Estado, en modo alguno conlleva una infracción de alcance constitucional"*. Además, apostilla diciendo que *"carecería de sentido, con el fin de sostener la validez de la diligencia de la prueba, la exigencia de que la autorización del agente encubierto se produzca a ciegas, con exclusión de cualquier contacto previo entre la persona que va a infiltrarse en la organización y quienes aparecen como miembros sospechosos de una red delictiva"*.

La autorización judicial que habilita al agente encubierto informático, por sí sola, no abre la puerta a la investigación. Dicha autorización, tiene que producirse una vez se tengan indicios mínimos de la actividad delictiva y cuando se hayan asentado unos lazos de confianza suficientes de modo que contribuyan al buen resultado de la investigación. Todo ello se puede enmarcar en los contactos previos con el investigado.

5.2.- CIBERPATRULLAJE

En los canales abiertos al intervenir bajo un "nickname", nombre ficticio -apodo- que un usuario utiliza para ser identificado en un servicio de la red, apenas existen identidades reales entre aquellos que son habituales de esos canales. Dentro de ellos se produce la investigación tecnológica o también llamado ciberpatrullaje, es decir, la prevención, investigación, práctica

[23] STS 767/007, de 3 de octubre, Sala Segunda de lo Penal; STS 292/2008, de 28 de mayo, Sala Segunda de lo Penal (disponibles en https://supremo.vlex.es/vid/facilitacion-pornografia-infantil-p-31969904; https://supremo.vlex.es/vid/facilitacion-pornografia-infantil-internet-42922794; última visita 30 de mayo de 2019).

[24] ZARAGOZA TEJADA J.I., "La modificación operada por la Ley 13/2015. El agente encubierto informático" p.12, *(disponible en* https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Zaragoza%20Tejada,%20Javier%20Ignacio.pdf?idFile=d16b7d76-2654-4b4e-abdf-b00f2540d57b ; última consulta 13 de abril de 2019).

[25] STS de 28 de junio de 2013, 3693/2013 - Recurso de Nicanor 2.B (disponible en: http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=6796422&links=Agente%20encubierto&optimize=20130715&publicinterface=true; última consulta 25 de abril de 2019).

de actuaciones de investigación dentro de la red, en canales abiertos donde no es necesaria una identificación real. De este modo, la figura del agente encubierto informático quedará fuera de aquellos canales de comunicación de carácter abierto tales como blogs, chats, foros, etc.

Por ello y amparado en las funciones que recoge el artículo 11 de la LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado, así como por lo dispuesto en el artículo 282 LECrim, estas acciones de ciberpatrullaje llevadas a cabo por los agentes de policía en los espacios abiertos con el fin de cumplir sus funciones y velar por la prevención o detección rápida de comportamientos delictivos, no requieren de ninguna autorización judicial.

5.3.- INTERCAMBIO Y ENVÍO DE ARCHIVOS ILÍCITOS

El artículo 288 bis 6) LECrim recoge como una de las actividades propias del agente encubierto informático el intercambio y envío de archivos ilícitos, es habitual que como modo de presentación y requisito de aceptación como nuevo miembro del grupo se le pida identificarse y, además, incluso compartir con el resto de los miembros archivos que demuestren su sensibilidad con el interés común del grupo. El problema radica en que esos archivos que han de intercambiarse y enviar deben ser creados con anterioridad.

Uno de los temas más controvertidos es la posibilidad del agente encubierto informático de aportar material ilícito al investigado. Ese material se tratará, en muchas ocasiones, de material pornográfico en que intervengan menores, y cuya mera creación supondría la comisión de un delito tipificado[26].

Dos son las alternativas doctrinales que en la práctica se barajan, si bien, ninguna está exenta de graves problemas. Por un lado, recurrir a material incautado en operaciones anteriores o

[26] Vid. sobre el particular RODRÍGUEZ CARO, M.V., "La infiltración policial: en el límite del Estado de Derecho. El inminente agente encubierto informático". (disponible en http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10222-la-infiltracion-policial:-en-el-limite-del-estado-de-derecho-el-inminente-agente-encubierto-informatico/; última consulta 2 de junio de 2019).

bien, la elaboración de material pornográfico ad hoc, protagonizado por actores mayores de edad, pero cuyo físico puede conducir a error sobre su verdadera edad[27].

Si se opta por la segunda de las soluciones, el supuesto pedófilo podrá argumentar que era conocedor de la mayoría de edad de los actores del archivo, aunque su apariencia fuera infantil. Además, si se trata de sujetos cuya apariencia crea dudas sobre su mayoría o no de edad, "por el juego del principio *in dubio pro reo*", podría llegarse también a una resolución absolutoria. Ya que, el acusado podría alegar su confusión sobre la edad de los sujetos presentes en los archivos[28].

Si se opta por la primera de las soluciones, esto es, recurrir a archivos pedófilos incautados en operaciones anteriores, debe realizarse atendiendo a criterios de excepcionalidad, necesidad y proporcionalidad. De tal forma que el fin perseguido, la importancia del delito y la envergadura de la operación policial, deben ser puestos en relación con las características del material que se vaya a poner en circulación.

5.4.- ANÁLISIS ALGORITMOS ASOCIADOS A ARCHIVOS ILÍCITOS

El artículo 282 bis 6) LECrim también recoge la posibilidad de "analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos". Esta expresión es más acertada que la plasmada en el Proyecto de Ley Orgánica de modificación de la LECrim. El interés que despierta este apartado es de gran calado ya que a través de su contenido y el examen de éste se pueden identificar los archivos.

En este campo se hizo una crítica concluyendo que la redacción no era del todo correcta, pues lo que interesa a los investigadores es el resultado de los algoritmos, ya que es lo que sirve para identificar los archivos informáticos, en concreto interesa el hash[29], el cual es la clave alfanumérica de los archivos.

[27] BUENO DE MATA, F (2012). "El Agente cubierto en internet: mentiras virtuales para alcanzar la justicia". (disponible en https://dialnet.unirioja.es/servlet/articulo;jsessionid=4A7CF70253AEF84F98D8F7F8C4BCD955.dialnet01?codigo=4036206; última consulta 30 de mayo de 2019).

[28] CAROU GARCÍA, S. "El agente encubierto como instrumento de lucha contra la pornografía infantil en internet. El guardián al otro lado del espejo". *Cuadernos de la Guardia Civil* Nº56. 2018 p.23-40.

[29]RUBIO ALAMILLO, J, define el término HASH como el código alfanumérico obtenido mediante un procedimiento matemático, el cual es único para el fichero, disco o memoria del cual se calcula.

En esta línea, es muy claro el Informe del Consejo Fiscal al Anteproyecto, para quien la identificación segura de archivos informáticos se realiza habitualmente mediante el hash. Señala éste que *"El hash es la clave alfanumérica resultante del análisis de los contenidos de cualquier archivo informático y su especificidad es tal que la más mínima alteración en el contenido del archivo determinaría la modificación de ese resultado hash. A su vez el término algoritmo se emplea para definir los pasos e instrumentos necesarios para obtener un resultado como es precisamente el hash"*. En consecuencia, para la Fiscalía lo relevante, en este sentido, no es el análisis de los algoritmos sino el análisis de los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos[30].

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

RUBIO ALAMILLO, J,[31] resume la actividad regulada en los apartados 6º) y 7º) del artículo 282 LECrim como la posibilidad de que un policía informático pueda enviarnos, si se tiene la sospecha de que estamos cometiendo un delito de cualquier tipo, uno o varios archivos ilícitos que posteriormente podrían ser encontrados en nuestro ordenador en una intervención domiciliaria. Dichos archivos, deben someterse a un inventario efectivo de ficheros ilícitos que vayan a ser utilizados y previamente auditados y almacenados correctamente en una base de datos segura junto a su correspondiente código hash para evitar su manipulación. Sin ese proceder, no sería posible distinguirlos del material que se hubiera obtenido del investigado sin esa ayuda policial.

[30] Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica de Modificación…, cit. p. 26-27.
[31] RUBIO ALAMILLO, J. "La informática en la reforma de la Ley de Enjuiciamiento Criminal", (disponible en https://peritoinformaticocolegiado.es/blog/la-informatica-en-la-reforma-de-la-ley-de-enjuiciamiento-criminal/; última consulta 8 de mayo de 2019).

VI.- AUTORIZACIÓN PARA LA INFILTRACIÓN

6.1.- LA AUTORIZACIÓN INICIAL DE LA INFILTRACIÓN

La actuación del agente encubierto informático va precedida de un auto judicial, concediendo la autorización por parte del Juez de Instrucción para la actividad del agente informático encubierto para la investigación correspondiente en un canal de comunicación cerrado. En ningún caso, será competente el Ministerio Fiscal para tal autorización.

La competencia del Ministerio del Interior quedará limitada a facilitar la identidad supuesta y los documentos necesarios para el desarrollo normal de las actividades correspondientes al agente encubierto informático. Nunca se podrá obligar a ningún funcionario público miembro de la Policía Judicial a actuar como agente encubierto.

En el auto se recogerán las medidas o pautas bajo las que el agente encubierto informático deberá cumplir su función. El juez instructor vigilará las actividades llevadas a cabo por el agente guiado siempre por el criterio de proporcionalidad como medida garantista de los Derechos Fundamentales.

Pese a los formalismos relativos a la autorización que se recogen en este capítulo VI, la condición formal de agente encubierto, atribuida mediante el auto judicial, es posterior al inicio de la actividad real de infiltración ya que son necesarios los contactos previos para que el agente vaya generando una confianza suficiente con los sujetos que se vayan a investigar. Siguiendo la jurisprudencia del Tribunal Supremo[32] se reconoce la plena validez probatoria de la información obtenida.

6.2.- FORMA Y CONTENIDO DE LA AUTORIZACIÓN

La resolución judicial que autoriza al agente encubierto informático incluirá la obligación de informar al agente de sus obligaciones o exigencias, así como de las competencias que tendrá bajo tal figura. Igualmente, se recogerá el marco en que se está autorizado para la utilización

[32] STS 575/2013, de 28 de junio (disponible en https://supremo.vlex.es/vid/449384218; última consulta 1 de junio de 2019); STS 277/2016, de 6 de abril (disponible en https://supremo.vlex.es/vid/633854037; última consulta 1 de junio de 2019).

de la identificación supuesta que le será concedida. Por ejemplo, si el agente informático tiene que crear un usuario en alguna red social, plataforma, etc. en el curso de su actividad, deberá remitir un acta al Juzgado de Instrucción que le autorizó informando de que esas pautas ya han sido llevadas a término.

También deberá recoger el auto que autoriza al agente encubierto la duración en el tiempo de dicha medida que, en principio, será para un plazo de tres meses como duración máxima inicial de la intervención, plazo que será susceptible de ampliación y prórroga, previa petición razonada por períodos sucesivos de igual duración, hasta un máximo temporal de dieciocho meses, siempre que subsistan las causas que la motivaron.

De esta forma se busca un equilibrio entre la necesidad de valerse de estas diligencias para la investigación de los delitos más graves para la sociedad y la importancia de definir unos límites cronológicos que no prolonguen de forma innecesaria la interferencia de los poderes públicos en la privacidad de los ciudadanos afectados por la medida[33].

Cabe recordar el deber de información recogido en la LECrim exigido al agente encubierto informático para con el Juez Instructor que le autorizó ya que según el artículo 282bis 1) LECrim, el agente encubierto informático deberá poner en conocimiento del autorizante la información que se vaya obteniendo en el curso de su actividad pese a que por el contrario no se indica en el precepto legal ninguna frecuencia con la que deba darse dicho deber de información.

Dentro del protocolo establecido en la Exposición de Motivos y con el principio de proporcionalidad como pilar fundamental para evitar en lo posible una vulneración excesiva de los derechos fundamentales del investigado y con el fin de asegurar la autenticidad e integridad de los soportes puestos a disposición del juez, se impone la utilización de un sistema de sellado o firma electrónica que garantice la información volcada desde el sistema central.

[33] Apartado IV de la exposición de motivos de la Ley Orgánica 13/2015 (BOE 6 de octubre de 2015).

En la Sentencia de la Sala de lo Penal de la Audiencia Nacional 1519/2018, de 26 de abril, se resumen muy bien las condiciones que debe recabar la autorización que media para la actuación del agente encubierto informático:

"1.- Autorizar al funcionario habilitado para poder intercambiar, en el periodo habilitado, intercambiar y enviar por sí mismo archivos ilícitos por razón de su contenido.
2.- Mantener secreta en pieza separada que quedará en poder del Letrado de la Administración de Justicia la resolución habilitante;
3.- Grabar íntegramente las conversaciones en el soporte correspondiente que se remitirá al juzgado donde constaran las grabaciones e imágenes con las transcripciones de interés;
4.- En el caso de que la investigación pueda afectar a los derechos fundamentales, el agente deberá solicitar del organismo judicial competente las autorizaciones que establezca la Constitución y la ley.
5.- Deberán adoptarse las debidas medidas de control para asegurarse que no se producirá ningún comportamiento por parte del agente que pueda constituir una provocación al delito y 6.- Toda la información que obtenga el agente encubierto informático deberá ser puesta en conocimiento del juzgado a la mayor brevedad para valorar su conformidad con el artículo 282 bis de la LECrim"[34].

También es necesaria una autorización judicial para la obtención de imágenes y grabación de conversaciones entre el agente e investigado, tal como se reconoce en el apartado 7º) del artículo 282 bis de la LECrim y siempre teniendo presente el test de proporcionalidad, idoneidad y necesidad, equilibrio entre el derecho lesionado y la ventaja obtenida, etc., ya que serían acciones vulneradoras, por ejemplo, del derecho al secreto de comunicaciones reconocido en el artículo 18 CE[35].

Entiende CONDE-PUMPIDO P. [36] que, se trata de una previsión legal específica al margen de la regulación general prevista en el capítulo VI de la LECrim referente a la captación y

[34] SAN 1519/2018, Sala de lo Penal, 26 de abril, (FJ1º) (disponible en http://www.poderjudicial.es/stfls/AUDIENCIA%20NACIONAL/JURISPRUDENCIA/AN%20Penal%2026%20abril%202018.pdf; última consulta 16 de mayo de 2019).
[35] ZARAGOZA TEJADA, J.I., "La modificación operada por la Ley 13/2015..." cit. p. 20.
[36] CONDE PUMPIDO, P. "El agente encubierto en la legislación española" p. 12 (disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20Conde-Pumpido%20Garc%C3%ADa,%20Paloma.pdf?idFile=bb24f82f-7461-4a13-ab8f-8d7de8f91f80; última consulta 30 de mayo de 2019).

grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, permitiendo complementar el resto de las medidas con la obtención de imágenes, incluso mediante la entrada en domicilio o espacio destinado al ejercicio de la privacidad.

Esto se puede justificar ante los límites estrictos que plantea el artículo 588 quater) LECrim, junto a los exigentes requisitos que conlleva el artículo 588 bis c) LECrim. Esta regulación del artículo 282 bis 7) LECrim se entiende que viene a cubrir la espontaneidad e informalidad de algunos encuentros entre el agente encubierto informático y el investigado, en espacios abiertos o no y probablemente en ocasiones con nuevos intervinientes.

Todas estas características harían que el rígido protocolo o los fuertes requisitos planteados en el capítulo VI fueran inviables y, por tanto, se entiende que viene a flexibilizar las exigencias antes unos supuestos tan cambiantes, ya que en caso de no existir esa versatilidad sería extremadamente complicado conseguir una autorización para cada encuentro.

En el supuesto de que fuera necesario que el agente encubierto informático grabase o captara imágenes o conversaciones mediante un dispositivo de grabación, que porte el agente encubierto informático, serán necesarias sendas autorizaciones judiciales del Juzgado de Instrucción correspondiente[37].

El agente encubierto informático podrá actuar en el marco de cualquiera de las siguientes funciones:

a) Enviar archivos que puedan ser ilícitos por su materia siempre y cuando rija el principio de proporcionalidad y legitimidad constitucional. Posteriormente, se recogerá como puede colisionar esta facultad con el concepto de provocación.
b) Grabación tanto de imagen como sonido o conversaciones mantenidas con el investigado.
c) Análisis de los archivos mediante algoritmos para investigar su procedencia, así como el rastro que hayan dejado o el recorrido de estos.

[37] Artículo 282 bis) apartado 7LECrim. *"En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio".*

ZARAGOZA TEJADA, J, [38] recalca que no hay ninguna regulación o protocolo sobre qué hacer con estos materiales ilícitos que se ponen en conocimiento del tribunal y que puede echarse en falta el establecimiento de mecanismos que permitan la recuperación integra del material aportado una vez enviado por el agente encubierto informático. Esto resultaría de vital necesidad, habida cuenta los intereses y derechos en juego que pueden quedar en peligro si se pierde el control del material difundido.

VII.- PRINCIPIOS BÁSICOS EN LA ACTUACIÓN DEL AEI

Para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple las tres siguientes condiciones siguiendo la línea marcada por el Tribunal Constitucional en su STC 186/2000[39]:

"1.- Si la medida acordada puede conseguir el objetivo propuesto (juicio de idoneidad).

2.- Si es necesaria en el sentido de que no exista otro medio más moderado para conseguir el fin propuesto con igual eficacia (juicio de necesidad); y

3.- Si la medida es equilibrada, es decir, que el beneficio que vaya a obtenerse debe ser superior al perjuicio causado por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto".

Dice el artículo 588 bis a 1) LECrim *"que durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida".*

7.1.- PRINCIPIO DE ESPECIALIDAD

El principio de especialidad se basa en que no podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva. Es decir, para cumplir este requisito del test de legitimidad la medida no podrá tener

[38] ZARAGOZA TEJADA, J.I., "La modificación operada por la Ley 13/2015…" cit. p. 25.
[39] STC 186/2000, de 10 de julio (FJ6) (disponible en https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4170; última consulta 2 de junio de 2019).

como objeto la mera actividad prospectiva sobre un supuesto delito sin base objetiva que justifique la actividad del agente encubierto informático. Siguiendo el artículo 588 bis a.2.) LECrim, se exige que la medida esté relacionada con la investigación de un delito concreto.

7.2.- PRINCIPIO DE IDONEIDAD

El principio de idoneidad define el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad[40]. Quiere decir esto que debe existir una relación entre el medio utilizado y el fin pretendido.

7.3.- PRINCIPIO DE EXCEPCIONALIDAD Y NECESIDAD

En cuanto a los principios de excepcionalidad y necesidad, solamente podrá aplicarse la medida cuando no existan otras alternativas que fueran menos lesivas con los derechos fundamentales del investigado y resultaran igual de útiles para la investigación o bien cuando sea ineludible para el esclarecimiento, averiguación de su paradero, etc. como recoge el artículo 588 bis a 4) de la LECrim.

Con mayor precisión, el principio de necesidad o principio de intervención mínima es la circunstancia que hace de límite y control al posible exceso de la medida en cuanto que pretende un equilibrio de los derechos fundamentales frente la afectación de éstos a través de medidas excesivas. De este modo, se pretende que se apliquen aquellas medidas menos lesivas para los derechos fundamentales y que, sin embargo, alcancen el mismo fin.

El principio de excepcionalidad pretende resaltar que la medida no es un medio normal de investigación, sino excepcional en la medida que supone el sacrificio de un derecho fundamental de la persona, por lo que su uso debe efectuarse con carácter limitado, ello supone que ni es tolerable la petición sistemática en sede judicial de tal autorización, ni menos se debe conceder de forma rutinaria. Por ello, este último principio de excepcionalidad se completa con los principios anteriores formando un todo inseparable, que actúa como valladar ante el riesgo de expansión que suele tener todo lo excepcional[41].

[40] Artículo 588 bis a 3 LECrim.
[41] STS 746/2014, 13 de noviembre de 2014, Sala Segunda de lo Penal (disponible en https://supremo.vlex.es/vid/550867582; última consulta 9 de mayo de 2019).

7.4.- PRINCIPIO DE PROPORCIONALIDAD

Por último, el principio de proporcionalidad, recogido en el artículo 588 bis a) 5 LECrim establece que *"las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".*

El artículo 1.1 de la CE proclama que España se constituye en un Estado social y democrático de Derecho, que propugna como valores superiores de su ordenamiento jurídico la libertad, la justicia, la igualdad y el pluralismo político. Este artículo reconoce la libertad como valor supremo y fija los pilares sobre los que se asentará el Estado a la vez que pone límites y/o pautas para el ejercicio del ius puniendi por parte del Estado. Igualmente, se complementa de la referencia del artículo 10.2 CE[42] a los artículos 10.2 y 18 del Convenio Europeo para la Protección de los Derechos Fundamentales y las Libertades Públicas[43].

El principio de proporcionalidad en sentido estricto es el tercer subprincipio del principio constitucional de prohibición de exceso o proporcionalidad en sentido amplio y se aplica, una vez aceptada la idoneidad y necesidad de una medida, con el fin de determinar, mediante la utilización de las técnicas del contrapeso de bienes o valores y la ponderación de intereses, según las circunstancias del caso concreto, si el sacrificio de los intereses individuales que comporta la injerencia guarda una relación razonable o proporcionada con la importancia del interés público que se trata de salvaguardar.

---

[42] Artículo 10.2 CE *"Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España".*

[43] Artículo 10.2 Convenio Europeo para la Protección de los Derechos Fundamentales y las Libertades Públicas *"El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial.*
Artículo 18 Convenio Europeo para la Protección de los Derechos Fundamentales y las Libertades *"Las restricciones que, en los términos del presente Convenio, se impongan a los citados derechos y libertades no podrán ser aplicadas más que con la finalidad para la cual han sido previstas".*

Si el sacrificio resulta excesivo deberá considerarse inadmisible, aunque satisfaga el resto de los presupuestos y requisitos derivados del principio de proporcionalidad[44].

Consecuencia de lo anterior, el principio de proporcionalidad debe atenderse en cada caso concreto, es decir, el Juez ponderará en cada supuesto si el sacrificio temporal del derecho fundamental es mayor al beneficio que se obtendrá. Por tanto, corresponde al Juez en cada caso el poner los criterios legales para la ponderación ya que este principio tiene carácter jurisprudencial[45].

Si bien es cierto que la legislación dicta ciertas pautas para una correcta ponderación para encontrar el equilibrio: gravedad del hecho, trascendencia social, el ámbito tecnológico en el que se hayan producido, la intensidad de los indicios que se tenga o la relevancia del resultado perseguido con la restricción del derecho. Cuantas más pautas asistan en el proceso de ponderación mayor proporcionalidad recaerá sobre la medida adoptada y, por tanto, mayor equilibrio. Estos principios generales básicos en la actuación del agente encubierto informático están reflejados en el artículo 588bis a) de la Ley de Enjuiciamiento Criminal[46].

VIII.- RESPONSABILIDAD AGENTE ENCUBIERTO INFORMÁTICO

El control de la proporcionalidad en cuanto a la actuación del agente encubierto informático es fundamental para la determinación de si ese ejercicio de investigación ha sido equitativo con los posibles derechos lesionados. Pese a esta afirmación, en la Constitución, no hay mención a un principio de proporcionalidad como criterio para determinar con carácter general los límites de los derechos o como canon para determinar la legitimidad de la intervención de los poderes públicos en la esfera de los derechos y libertades públicas[47].

---

[44] GONZÁLEZ-CUÉLLAR SERRANO, N. "El principio de proporcionalidad en el derecho procesal español", *Cuadernos de Derecho Público nº 5. Septiembre-Diciembre 1998.* (disponible en https://previa.uclm.es/area/procesal/Proporcionalidad.htm; última visita 15 de mayo de 2019).

[45] VELASCO NÚÑEZ, E. *Delitos tecnológicos. Definición, investigación y prueba en el proceso penal*. Sepin, Madrid. (2016), p. 69ss.

[46] *"Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".*

[47] ROCA TRÍAS, E; AHUMADA RUÍZ, Mª A., "Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española" *Reunión de Tribunales Constitucionales de Italia, Portugal y España,*

La actuación del agente encubierto informático deberá ajustarse al test de legitimidad constitucional que pretende proteger la afectación a los Derechos Fundamentales. Esto es, deberá argumentar la idoneidad de la medida, es decir, justificar la actuación del agente encubierto informático, su necesidad y el debido equilibrio entre el sacrificio lesivo padecido de los derechos fundamentales y la ventaja que se logrará con dicha lesión del derecho o derechos fundamentales para la investigación[48].

El artículo 282bis 5 LECrim establece una cláusula de exención de responsabilidad del agente encubierto, aunque será necesaria la concurrencia de una serie de requisitos: que las actuaciones desarrolladas sean consecuencia necesaria para la investigación; que guarden la debida proporcionalidad con la finalidad de ésta y no constituyan una provocación al delito. Sin embargo, sí responderá por aquellas actuaciones que no estén relacionadas con la investigación. También responderán penalmente aquellos agentes que actúen de forma encubierta sin someterse a los formalismos del artículo 282bis LECrim.

En los siguientes subapartados se van a desglosar los aspectos más relevantes de las posibles responsabilidades en que el agente encubierto informático puede incurrir.

8.1.- RESPONSABILIDAD PENAL

El agente encubierto informático responderá de aquellas actividades que no sean consecuencia necesaria de la investigación, que sean desproporcionadas con la finalidad de ésta, debiendo ser el infiltrado el que realice la ponderación en cada caso concreto[49].

Pese a la cláusula de exención de responsabilidad criminal al agente encubierto, el apartado 5 del artículo 282bis LECrim, prevé el procedimiento para exigir responsabilidad penal al agente encubierto por sus actuaciones. El juez competente que conozca de la causa requerirá un informe a quien haya autorizado la identidad supuesta del agente encubierto, en atención al cual resolverá lo que a su criterio proceda.

Roma, octubre 2013 (disponible en https://www.tribunalconstitucional.es/ActividadesDocumentos/2013-10-24-00-00/2013-PonenciaEspaña.pdf, última consulta 13 de abril de 2019).

[48] STC Sala Primera, 29 de mayo de 2000, STC 136/2000, FJ 4º, (disponible en https://hj.tribunalconstitucional.es/es/Resolucion/Show/4120, última visita 16 de abril de 2019).

[49] ZAFRA ESPINOSA DE LOS MONTEROS, R, "El agente encubierto en el ordenamiento jurídico español", *Publicaciones del Portal Iberoamericano de las Ciencias Penales. Instituto de Derecho Penal Europeo e Internacional*. Universidad de Castilla La Mancha. p. 20 *(disponible en www.tirantonline.com; última visita 28 de mayo de 2019).*

PERALS CALLEJA, J.[50] hace referencia a esa cláusula de exención de responsabilidad penal diciendo que en caso contrario difícilmente un funcionario policial asumiría participar en tales investigaciones. Claro está que a los efectos de que el precepto no sea una "carta en blanco" se establece la limitación mencionada con anterioridad (que los actos sean consecuencia necesaria de la investigación, sean proporcionales y no constituyan un delito provocado).

8.2.- RESPONSABILIDAD CIVIL

En cuanto a la responsabilidad civil que pudiera derivarse de la comisión de un delito (responsabilidad civil extracontractual) teniendo en cuenta el artículo 1902 del Código Civil[51], el agente encubierto quedará exento de responsabilidad si su conducta era necesaria y proporcional para la investigación en curso. En caso de que no se ajuste a estos requisitos, el agente responderá civilmente frente al Estado y/o terceros perjudicados, y en caso de no hacerlo, responderá subsidiariamente el Estado.

Por los actos o negocios jurídicos (responsabilidad civil contractual), que hubiera realizado el agente encubierto bajo su identidad supuesta, y atendiendo al artículo 1911 del Código Civil[52], responderá el propio agente. En caso de ser necesarios esos actos para el normal desarrollo de las investigaciones, al igual que en la responsabilidad penal o civil extracontractual, estará exento de responsabilidad.

Si por el contrario se da una responsabilidad civil contractual por parte del agente, el dilema será contra qué identidad debe reclamar el tercero perjudicado. En caso de que la investigación esté activa, dicha reclamación se dirigirá contra la identidad supuesta del agente encubierto.

Sin embargo, si la investigación ha concluido, carecería de sentido reclamar a una persona "encubierta" o cuya identidad no existe. El acreedor perjudicado tendrá que ser informado

[50] PERALS CALLEJA, J. "El agente encubierto. La figura del arrepentido. Protección de testigos. Entrada y registro. Apertura de correspondencia". (disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/PONENCIA%20JOS%C3%89%20PERALS%20CALLEJA.pdf?idFile=73fec82f-93b7-4229-ada1-7d3a85ebdfaf; última consulta 30 de mayo de 2019).

[51] Artículo 1902 Código Civil: *" El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado".*

[52] Artículo 1911 Código Civil: *"Del cumplimiento de las obligaciones responde el deudor con todos sus bienes, presentes y futuros".*

acerca de a quién debe dirigir su reclamación. La responsabilidad civil contractual será del agente con el tercero perjudicado, y subsidiariamente, podrá dirigirse contra el Estado[53].

8.3.- RESPONSABILIDAD DISCIPLINARIA O ADMINISTRATIVA

El agente infiltrado es un funcionario público y como tal debe regirse por su régimen de responsabilidad. En este apartado se tiene que prestar especial atención al artículo 7b) de la LO 4/2010, 20 de mayo del Régimen Disciplinario del Cuerpo Nacional de Policía *"Haber sido condenado en virtud de sentencia firme por un delito doloso relacionado con el servicio o que cause grave daño a la Administración o a las personas".*

Según CARDOSO PEREIRA F.[54], la irrogación de la sanción administrativa queda condicionada a la decisión final tomada en el proceso penal, surgiendo de este modo una cuestión prejudicial devolutiva administrativa en el proceso penal. Esta casuística nos lleva a plantearnos si en este caso de sanción concomitante se estaría violando la regla del principio del *non bis in idem.*

No hay una misma interpretación a este respecto porque la sanción administrativa queda vinculada a la decisión tomada en el proceso penal. Sin embargo, lo más acertado siguiendo el criterio del Tribunal Constitucional y ajustado al principio *non bis in idem,* es que la legislación de la Función Pública permitiera a la Administración, tras la condena de un funcionario, imponerle una sanción administrativa, en tanto en cuanto hubiera lugar a una compensación de las sanciones ya que las responsabilidades penales y administrativas son distintas y autónomas, presentando sus propias especificidades y particularidades, no siendo correcta la invocación del principio de la prohibición del *non bis in idem*[55].

[53] ZAFRA ESPINOSA DE LOS MONTEROS, R. *El policía infiltrado. Los presupuestos jurídicos en el proceso penal español.* Tirant lo Blanch, Valencia, 2010. p.422.
[54] CARDOSO PEREIRA, F. "Agente encubierto y proceso penal garantista: límites y desafíos" p. 312ss. Salamanca (2012). (disponible en https://gredos.usal.es/jspui/bitstream/10366/121134/1/DDAFP_CardosoFlavio_Tesis.pdf; última consulta 30 de mayo de 2019).
[55] CARDOSO PEREIRA, F. "Agente encubierto y proceso…" cit. p.313

Esta postura seguida por CARDOSO PEREIRA choca con la jurisprudencia del Tribunal Europeo de Derechos Humanos[56], que sí considera que se infringe el principio *non bis in idem* y procede anulando la sanción posterior.

IX.- EFECTOS PROCESALES DE LA INFILTRACIÓN

9.1.- LA DECLARACIÓN EN LA FASE DE INSTRUCCIÓN

El agente encubierto deberá poner en conocimiento del juez instructor que autorizó su actuación toda la información que vaya obteniendo a la mayor brevedad posible, según se recoge en el último apartado del artículo 282 bis LECrim. Lo habitual será que el infiltrado se relacione con los mandos policiales que diseñaron la operación y que éstos lo pongan en conocimiento del órgano competente.

La información obtenida en su integridad a lo largo de la instrucción debe ser puesta en conocimiento del Juzgado de Instrucción ya que dicha información puede servir de indicios para la adopción de otras diligencias de investigación complementarias de la infiltración policial[57].

En la fase instructora no debiera solicitarse la declaración del agente encubierto puesto que el juez tiene conocimiento de toda la información que ha ido obteniendo, y nada nuevo aportaría su comparecencia, salvo riesgo para su persona y pérdida del carácter reservado de su identidad[58].

9.2.- LA DECLARACIÓN TESTIFICAL EN LA FASE ORAL

Uno de los mayores problemas que pueden plantearse en cuanto a la figura del agente encubierto informático son las vías a través de las cuales los medios de prueba obtenidos pueden ser introducidos en el acto del juicio oral[59].

---

[56] STEDH, caso Sallen c. Austria, de 6 de junio de 2002 (TEDH 2002/35; caso CF c. Austria, de 30 de mayo de 2002 (TEDH 2002/35), (disponible en http://lawcenter.es/w/file/download/66104; última consulta 1 de junio de 2019).
[57] ZAFRA ESPINOSA DE LOS MONTEROS, R. "El agente encubierto en el ordenamiento…" cit. p.17.
[58] CONDE PUMPIDO, P. "El agente encubierto en la legislación española" cit. p.16.
[59] ZARAGOZA TEJADA, J.I. "La modificación operada por la Ley 13/2015…" cit. p. 29.

La información más importante sobre la investigación la obtendrá el agente encubierto informático por aquello que haya visto u oído. A este respecto, se convierte en testigo una vez finalizada su actividad infiltrada. La información que éste obtenga deberá ser transmitida a quien sea el encargado de la dirección del proceso, sólo a partir de ese momento comenzará a tener relevancia judicial[60].

En primer lugar, se propone la declaración testifical del agente policial que ha actuado como agente encubierto informático, a través del interrogatorio, donde podrá poner de manifiesto todo lo que haya recopilado a lo largo de la investigación, así como todos los hechos de los que es conocedor. El material obtenido deberá ser aportado al juicio como prueba documental para que el tribunal lo pueda apreciar y valorar bajo los principios de inmediación y contradicción[61].

Además, en cuanto a la declaración del agente encubierto informático en juicio, el articulado del 282 bis) permitía mantener la identidad supuesta en la declaración testifical en el juicio, máxime, cuando con esto se pretende la constatación de que en la investigación no ha existido provocación.

Sin embargo, pese a que el punto 2º) de dicho artículo establece que podrá mantener la identidad supuesta, habrá que estar también a lo dispuesto en la Ley 19/1994 del 23 de diciembre, de protección de testigos y peritos, especialmente, a su artículo 4.3.[62]. Además de este primer mecanismo, se puede incluso solicitar la identidad del testigo oculto, en protección del derecho de defensa regulado expresamente en el artículo 24.2 de la CE y en el artículo 6.3 d) del Convenio Europeo de Derechos Humanos.

Un tercer mecanismo es la declaración de testigos de referencia en el acto del juicio oral. Es decir, que otro agente de policía, ajeno a la infiltración declare en plenario aquello que le contó el agente encubierto. La LECrim regula la utilización de los testigos de referencia en el artículo 710.

---

[60] GASCÓN INCAHUSTI, F., *Infiltración policial y <agente encubierto>*, Comares, Granada, 2001, p. 257.
[61] ZARAGOZA TEJADA, J.I. "La modificación operada por la Ley 13/2015…*".* cit. p. 29.
[62] *"Si cualquiera de las partes solicitase motivadamente en su escrito de calificación provisional, acusación o defensa, el conocimiento de la identidad de los testigos o peritos propuestos, cuya declaración o informe sea estimado pertinente, el Juez o Tribunal que haya de entender la causa, en el mismo auto en el que declare la pertinencia de la prueba propuesta, deberá facilitar el nombre y los apellidos de los testigos y peritos, respetando las restantes garantías reconocidas a los mismos en esta Ley".*

Por último, resaltar que con la declaración testifical se persigue constatar que no ha habido provocación. Con este artículo se trata de salvaguardar el derecho de defensa y proteger el principio de contradicción que conforma el derecho a la tutela judicial efectiva que se consagra en el artículo 24 de nuestra Carta Magna como un derecho fundamental[63].

Pese a que la redacción literal del artículo 282bis 2) LECrim reconoce la posibilidad de que el agente encubierto mantenga la identidad falsa en el juicio oral, también hace una mención específica refiriéndose al apartado 1º), dejando, por el contrario, de especificar si el resto de los apartados, concretamente, el 6º) y 7º) deberán de guiarse bajo las mismas directrices o si, por el contrario, al no ir al caso concreto, se debe entender que no mantendría la identidad supuesta.

Ante este interrogante, el Fiscal ZARAGOZA TEJADA J[64] hace una interpretación de la norma en la que deja fuera al agente encubierto informático a la hora de mantener su identidad supuesta, aunque entiende que debiera de interpretarse sistemáticamente. Funda esa interpretación en que mantener la identidad falsa del agente encubierto informático carece de la justificación que tenía esa garantía de preservar la verdadera identidad del agente encubierto en su concepción clásica, ya que se infiltraba en investigaciones dentro de organizaciones criminales y terroristas donde sí existía un verdadero riesgo de que posteriormente hubiera actos represivos y de venganza contra el agente infiltrado o bien contra su círculo más cercano.

9.3.- EFECTOS PROBATORIOS

Otro de los puntos clave en lo que se circunscribe al testimonio del agente encubierto informático es su eficacia probatoria. Como una primera aproximación a este punto, habrá que prestar atención al artículo 717 LECrim, donde se recoge que *"Las declaraciones de las autoridades y funcionarios de policía judicial tendrán el valor de declaraciones testificadas, apreciables como éstas según las reglas del criterio racional".*

[63] *"1.- Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión. 2.- Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia. La ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos".*

[64] ZARAGOZA TEJADA, J.I., "La modificación operada por la Ley 13/2015…" cit. p. 30.

El problema principal surge en aquellos casos en que el agente encubierto y siempre dentro de sus competencias, sea testigo de una confesión por parte del investigado. Aquí se confronta lo recogido anteriormente en el artículo 717 LECrim con la corriente jurisprudencial que en los últimos años ha considerado que la confesión efectuada por el investigado por un delito ante agentes de las Fuerzas y Cuerpos de Seguridad del Estado no pueden ser valoradas por los Tribunales a la hora de adoptar una resolución sobre el fondo del asunto[65].

Lo anterior se ve plenamente alineado con el acuerdo del Pleno no jurisdiccional de la Sala Segunda de fecha 3 de junio de 2015 donde se señala que *"Las declaraciones ante los funcionarios policiales no tienen valor probatorio. No pueden operar como corroboración de los medios de prueba, ni ser contrastadas por la vía del artículo 714 de la LECrim, ni cabe su utilización como prueba preconstituida en los términos del artículo 730 de la LECrim. Tampoco pueden ser incorporadas al acervo probatorio mediante la llamada como testigos de los agentes policiales que las recogieron.*

Sin embargo, cuando los datos objetivos contenidos en la autoinculpación son acreditados como veraces por verdaderos medios de prueba, el conocimiento de aquellos datos por el declarante, evidenciado en la autoinculpación, puede constituir un hecho base para legítimas y lógicas inferencias. Para constatar, a estos exclusivos efectos, la validez y el contenido de la declaración policial, deberán prestar testimonio en el juicio los agentes policiales que la presenciaron[66]*".*

Con todo esto, la principal vulneración posible a la que se podría hacer frente en el acto de juicio será el derecho a no declarar contra sí mismo, ya que es un principio recogido en el artículo 24 de la CE, amparado además como derecho fundamental.

Aquí habrá que valorar si existen más indicios que puedan ser prueba de cargo, excluyendo la obtención de una posible autoinculpación obtenida por esa grabación del agente encubierto, a la que se hacía referencia líneas arriba. En caso de que esa grabación sea la única prueba de la

[65] ZARAGOZA TEJADA, J.I. "La modificación operada por la Ley 13/2015…" cit. p. 31.

[66] Acuerdo del Pleno no jurisdiccional de la Sala Segunda, 3 de junio de 2015. (disponible en https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-P-2015-10049900500_ANUARIO_DE_DERECHO_PENAL_Y_CIENCIAS_PENALES_Acuerdos_del_Pleno_de_la_Sala_Segunda_del_Tribunal_Supremo_(año_2015); última consulta 16 de mayo de 2019).

actividad delictiva, al haberse conseguido con una vulneración de un derecho fundamental, no tendría validez, a tenor del artículo 11.1 LOPJ, ya que *"En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales".*

Otro de los aspectos relativos es la ilicitud de la prueba regulada en el artículo 11 LOPJ, reproducido en el párrafo anterior, que la vincula a la limitación de derechos fundamentales o libertades públicas.

La consecuencia de inmediata de la ilicitud es la imposibilidad de utilizar lo obtenido mediante el acto nulo de forma directa o indirecta. En los supuestos de infiltración policial, afirma ZAFRA ESPINOSA DE LOS MONTEROS, R.[67], la nulidad probatoria puede venir por la autorización inicial, bien porque se ha actuado sin la correspondiente habilitación para el agente encubierto informático o porque se ha autorizado sin respetar los parámetros exigidos por la ley y que he desarrollado anteriormente. Al entenderse que con la infiltración policial se están lesionando derechos fundamentales, toda prueba obtenida en la investigación devendrá nula.

En todos los casos en que se produzca una ilicitud probatoria de las recogidas en el artículo 11 LOPJ no sólo se tendrá como nula esa prueba, sino que todas las que deriven de ella serán también ilícitas siguiendo la doctrina de los efectos reflejos de la prueba ilícita o también estudiada como doctrina de los frutos del árbol envenenado[68].

[67] ZAFRA ESPINOSA DE LOS MONTEROS R. "El agente encubierto en el ordenamiento…" cit. p. 20
[68] PÉREZ VAQUERO, C. "La doctrina de los frutos del árbol envenenado". (disponible en http://archivodeinalbis.blogspot.com/search?q=envenenado).

X.- CONCLUSIONES

Tras tiempo de análisis, estudio y lecturas de diferentes artículos, revistas y sentencias he podido profundizar en las medidas de investigación tecnológica, especialmente, en la figura del agente encubierto informático que centra este Trabajo Fin de Grado.

Primera. - La concepción clásica del agente encubierto se vio sustancialmente desvirtuada del mundo físico con la Ley Orgánica 13/2015, mediante la cual, con la introducción de dos nuevos apartados al artículo 282 bis, se forjó el agente encubierto informático, también llamado virtual u online, realidad que quedaba lejos del concepto tradicional.

Segunda. - El criterio de organización criminal como requisito para la actuación del agente encubierto informático creo que ha quedado desfasado y se podría haber aprovechado esta reforma para actualizar los términos.

Tercera. - Las competencias para actuar como agente encubierto informático son exclusivas de la Policía Judicial. Debe de existir gran coordinación y colaboración entre el juez instructor que autoriza dicha medida de investigación con quien va a llevarla a cabo.

Cuarta. - La figura del agente encubierto informático quedará ligada a los canales de comunicación cerrados donde se necesita una identidad supuesta para poder acceder. Por el contrario, cuando se trate de una investigación en canales abiertos, donde se pueda actuar bajo un apodo y por tanto, no se produce engaño, se encaja en labores de prevención de delitos o cualquier otra competencia de las Fuerzas y Cuerpo de Seguridad del Estado. A esta actividad de prevención la conocemos como ciberpatrullaje.

Quinta. - Especial cuidado, desde mi punto de vista, requiere el envío de archivos ilícitos para que esta práctica no pueda alegarse como una provocación y que, por lo tanto, derive en una nulidad de las actuaciones y se malogre la investigación.

Sexta.- Con los continuos avances tecnológicos y las nuevas formas de interacción a nivel global, resulta necesario adaptar periódicamente la legislación en lo referente a la

investigación para que, en la mayor medida posible, avance en paralelo a la realidad y no se produzcan vacíos legales que puedan dejar huérfano de investigación a las nuevas formas de delinquir que llevan parejos dichos avances tecnológicos y además, con un carácter fundamental de anonimato que hace muy complicado identificar a los autores del delito.

Séptima. - Entiendo que era vital la regulación introducida por la LO 13/2015, aunque creo que resulta deficiente en cuanto a su redacción y concreción. Además, tan sólo cuatro años después de dicha reforma, hay aspectos que ya debieran ser actualizados, como, por ejemplo, lo relativo a los delitos que se puedan circunscribir respecto a las criptomonedas o las últimas novedades dentro del mundo virtual.

Octava. - Pienso que el protocolo debiera ser más concreto de modo que se acotara la discrecionalidad del juez instructor que debe autorizar la actuación del agente encubierto informático para llevar a cabo sus labores de investigación. Igualmente, opino que las labores de información al juez instructor debieran estar también más reguladas.

Novena. - En cuanto a los delitos en que pueda actuar el agente encubierto informático creo que debería tener competencia a todos aquellos que se hayan cometido en el mundo virtual, o a través de internet.

Décima. - A la hora de legislar temas tan específicos debe darse una colaboración con expertos de la materia que se va a regular, ya que si no encontramos ambigüedades o incoherencias técnicas.

XI.- BIBLIOGRAFÍA

Acuerdo del Pleno no jurisdiccional de la Sala Segunda, 3 de junio de 2015. (disponible en https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-P-2015-10049900500_ANUARIO_DE_DERECHO_PENAL_Y_CIENCIAS_PENALES_Acuerdos_del_Pleno_de_la_Sala_Segunda_del_Tribunal_Supremo_(año_2015); última consulta 16 de mayo de 2019).

Agente encubierto informático. Reforma LECrim. Con José Ramón Navarro (disponible en https://www.youtube.com/watch?v=KgtO0lrmE00 ; última consulta 17 de mayo de 2019).

BUENO DE MATA, F., "El Agente encubierto en internet: mentiras virtuales para alcanzar la justicia". (disponible en https://dialnet.unirioja.es/servlet/articulo;jsessionid=4A7CF70253AEF84F98D8F7F8C4BCD955.dialnet0 1?codigo=4036206; última consulta 30 de mayo de 2019).

CARDOSO PEREIRA, F., "Agente encubierto y proceso penal garantista: límites y desafíos" Salamanca (2012). (disponible en https://gredos.usal.es/jspui/bitstream/10366/121134/1/DDAFP_CardosoFlavio_Tesis.pdf; última consulta 30 de mayo de 2019).

CAROU GARCÍA, S. "El agente encubierto como instrumento de lucha contra la pornografía infantil en internet. El guardián al otro lado del espejo". *Cuadernos de la Guardia Civil* Nº56. 2018.

CONDE-PUMPIDO, P, "El agente encubierto en la legislación española" *(disponible en* https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20Conde-Pumpido%20Garc%C3%ADa,%20Paloma.pdf?idFile=bb24f82f-7461-4a13-ab8f-8d7de8f91f80 *;* última consulta 30 de mayo de 2019).

DE DIEGO DÍEZ, "El proceso penal" *(disponible en www.tirantonline.com ; última consulta 27 de mayo de 2019).*

DE LA ROSA CORTINA, J.M., *Los delitos de pornografía infantil. Aspectos penales, procesales y criminológicos*, Tirant lo Blanch, Valencia, 2011.

DEL POZO PÉREZ, M., "El agente encubierto como medio de investigación de la delincuencia organizada en la ley de enjuiciamiento criminal española" *Criterio Jurídico*, Dialnet.

El agente policial encubierto en internet. Analiza el Prof. Ricardo Magaz. RTVCyL (disponible en https://www.youtube.com/watch?v=h23sobdqw0Q ; última consulta 17 de mayo de 2019).

EXPÓSITO LÓPEZ L., "El agente encubierto. The undercover agent". *Revista de Derecho UNED, Núm. 17, 2015.*

GARBERÍ A., abril 2016, "*Comentarios sobre el delito provocado*" (disponible en http://www.garberipenal.com/delito-provocado-practica-agente-encubierto/; última consulta 20 de abril de 2019).

GASCÓN INCAHUSTI, F., *Infiltración policial y <agente encubierto>*, Comares, Granada, 2001

GIMENO SENDRA, V., *Manual Derecho Procesal Penal*, Castillo de Luna Ediciones Jurídicas, Madrid, 2018.

GOICOECHEA. N." *España, tercer país del mundo en ciberataques"* (disponible en https://cadenaser.com/ser/2014/11/25/ciencia/1416920321_278876.html; última consulta 14 de abril de 2019).

GONZÁLEZ-CUÉLLAR SERRANO, N. *"El principio de proporcionalidad en el derecho procesal español", Cuadernos de Derecho Público nº 5. Septiembre-Diciembre 1998 (disponible en* https://previa.uclm.es/area/procesal/Proporcionalidad.htm; última consulta 15 de mayo de 2019).

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 (disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/INFORME_CF_MODIFICACIÓN_LECrim_23-01-2015.pdf?idFile=7c2cd525-01bf-4cc0-864a-29dc8ee0dae9; última consulta 5 de mayo de 2019).

JURADO FORTES, M., *"Agente encubierto informático"*, López de Lemus Abogados. (disponible en https://lopezdelemus.com/agente-encubierto-informatico/; última consulta 11/05/2019).

MARCHENA GÓMEZ, M., GONZÁLEZ CUELLAR SERRANO, N., *La reforma de la Ley de enjuiciamiento criminal en 2015*. Madrid, 2015

MONTÓN GARCÍA, M.L., "Agente provocador y agente encubierto: ordenemos conceptos*"*, *La Ley*, nº 4826, 1999.

PERALS CALLEJA, J. "El agente encubierto. La figura del arrepentido. Protección de testigos. Entrada y registro. Apertura de correspondencia". (disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/PONENCIA%20JOS%C3%89%20PERALS%20CALLEJA.pdf?idFile=73fec82f-93b7-4229-ada1-7d3a85ebdfaf; última consulta 30 de mayo de 2019).

PÉREZ VAQUERO, C. "La doctrina de los frutos del árbol envenenado". (disponible en http://archivodeinalbis.blogspot.com/search?q=envenenado).

RAIMÚNDEZ LÓPEZ, S., "Nuevas técnicas de investigación y su posible afectación a los derechos fundamentales: la figura del agente encubierto". *Universidad de Oviedo.*

RIFÁ SOLER, JM, "El agente encubierto o infiltrado en la nueva regulación de la Ley de Enjuiciamiento Criminal*", Revista del Poder Judicial, nº55, CGPJ, 1999*. SILVA SÁNCHEZ, JM. "La consideración del comportamiento de la víctima", en *Cuadernos del Consejo General del Poder Judicial (disponible en www.tirantonline.com ; última visita 28 de mayo de 2019).*

ROCA TRÍAS, E; AHUMADA RUÍZ, Mª. A., *"Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española" (disponible en* https://www.tribunalconstitucional.es/ActividadesDocumentos/2013-10-24-00-00/2013-PonenciaEspaña.pdf ; última consulta 13 de abril de 2019).

RODRÍGUEZ CARO, M.V., *"La infiltración policial: en el límite del Estado de Derecho. El inminente agente encubierto informático" (disponible en* http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10222-la-infiltracion-policial:-en-el-limite-del-estado-de-derecho-el-inminente-agente-encubierto-informatico/; última consulta 2 de junio de 2019).

RUBIO ALAMILLO, J. *"La informática en la reforma de la Ley de Enjuiciamiento Criminal",* (disponible en https://peritoinformaticocolegiado.es/blog/la-informatica-en-la-reforma-de-la-ley-de-enjuiciamiento-criminal/;última consulta 8 de mayo de 2019).

RUIZ ANTÓN, LF., *El agente provocador en el derecho penal*, Edersa, Madrid, 1982

SÁNCHEZ GÓMEZ, R., "El agente encubierto informático", *La Ley 842/2016*

VALIÑO CES, A., *"El proceso penal. Cuestiones fundamentales. La actuación del agente encubierto en los delitos informáticos tras la Ley Orgánica 13/2015"* Coord. Olga Fuentes Soriano. *(disponible en www.tirantonline.com ; última consulta 28 de mayo de 2019).*

VELASCO NÚÑEZ, E. *Delitos tecnológicos. Definición, investigación y prueba en el proceso penal*. Sepin, Madrid. (2016).

VILLAR FUENTES I, *"El agente infiltrado y las diligencias de investigación tecnológica",* Archivio penale 2017, nº 2, Dall´Europa (disponible en http://www.archiviopenale.it/File/Download?codice=4f03a98a-2ff7-4b47-beaf-f85630bbc39c ; última consulta 20 de abril de 2019).

VILLAR FUENTES I., *"El proceso penal. Cuestiones fundamentales, Reflexiones sobre el agente encubierto"* Coord. Olga Fuentes Soriano. *(disponible en www.tirantonline.com ; última visita 27 de mayo de 2019)*

ZAFRA ESPINOSA DE LOS MONTEROS, R, "El agente encubierto en el ordenamiento jurídico español", *Publicaciones del Portal Iberoamericano de las Ciencias Penales. Instituto de Derecho Penal Europeo e Internacional. Universidad de Castilla La Mancha (disponible en www.tirantonline.com; última visita 28 de mayo de 2019)*
Zafra Espinosa de los Monteros, R. *El policía infiltrado. Los presupuestos jurídicos en el proceso penal español.* Tirant lo Blanch, Valencia, 2010

ZAFRA ESPINOSA DE LOS MONTEROS, R. "Globalización y lucha contra las nuevas formas de criminalidad transnacional" (disponible en www.tirantonline.com; última consulta 1 de junio de 2019).

ZARAGOZA TEJADA, J. Y BERMÚDEZ GONZÁLEZ J. (2017). "Investigación tecnológica y derechos fundamentales". Cizur Menor (Navarra): Aranzadi-Thomson Reuters

ZARAGOZA TEJADA, J, *"La modificación operada por la Ley 13/2015. "El agente encubierto informático" (disponible en* https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Zaragoza%20Tejada,%20Javier%20Ignacio.pdf?idFile=d16b7d76-2654-4b4e-abdf-b00f2540d57b ; última consulta 13 de abril de 2019).

JURISPRUDENCIA:

Tribunal Constitucional:
STC 136/2000, 29 de mayo de 2000
STC 186/2000, de 10 de julio de 2000

Tribunal Supremo:
STS 746/2014, 13 de noviembre de 2014
STS 3693/2013, 28 de junio de 2013
STS 289/2015, de 28 de septiembre de 2015
STS 253/2015, de 24 de abril de 2015
STS 204/2013, de 14 de marzo de 2013
STS 575/2013, de 28 de junio de 2013

STS 277/2016, de 6 de abril de 2016
STS 863/2011, de 21 de julio de 2011
STS 395/2014, de 13 de mayo de 2014
STS 1140/2010, de 29 de diciembre de 2010
STS 289/2015, de 28 de septiembre de 2015
STS 767/2007, de 3 de octubre de 2007
STS 292/2008, de 28 de mayo de 2008
STS 345/2019, de 7 de febrero de 2019
STS 140/2019, de 13 de marzo de 2019

Audiencia Nacional:
SAN 1519/2018, de 26 de abril de 2018

Tribunal Europeo de Derechos Humanos
STEDH 2002/35, (Sección 1), de 2 julio 2002. Caso S.N. contra Suecia. Demanda núm. 34209/1996.

LEGISLACIÓN:

Constitución Española.

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, BOE 6 de octubre de 2015.

Acuerdo Europeo para la protección de los Derechos Fundamentales y las Libertades Públicas, BOE 6 de mayo de 1999.

Ley Orgánica 5/1999, de 13 de enero, de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves, BOE 14 de enero de 1999.

Ley Orgánica 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad, BOE 14 de marzo de 1986.

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, BOE 17 de septiembre de 1882.

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, BOE 2 de julio de 1985.

Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales, BOE 24 de diciembre de 1994.