COLEGIO UNIVERSITARIO DE ESTUDIOS FINANCIEROS

DOBLE GRADO EN DERECHO Y ADE

Trabajo Fin de GRADO

AGENTE ENCUBIERTO INFORMÁTICO

NUEVA MEDIDA DE INVESTIGACIÓN.

Autor: Escobar Rodríguez, María del Valle

Tutor: Dr. D. Jesús María Zarzalejos Nieto

Madrid, diciembre 2018

ÍNDICE

1. Introducción: Objeto del trabajo……4

2. Modificación de la Ley de Enjuiciamiento Criminal……5

3. Supuesto de hecho……8

4. El agente encubierto en internet ……9

   4.1. Definición……9
   4.2. Ámbito de actuación ……11
   4.3. Canales de comunicación cerrados ……13

5. Actuaciones del agente encubierto informático ……15

6. Delito provocado y agente provocador ……17

7. Medida restrictiva de derechos fundamentales ……22

   7.1. Principio de proporcionalidad ……23
   7.2. Otras observaciones sobre la Resolución judicial para autorizar la actuación del agente encubierto. ……26

8. Responsabilidad del agente encubierto ……29

9. Conclusiones……32

10. Bibliografía……34

ÍNDICE DE ABREVIATURAS

AEI: Agente Encubierto Informático

Art.: Artículo

CE: Constitución Española

LECrim: Ley de Enjuiciamiento Criminal

LO: Ley Orgánica

ss. : y siguientes

STS: Sentencia del Tribunal Supremo

1. INTRODUCCIÓN: OBJETO DEL TRABAJO

La sociedad del siglo XXI, también llamada sociedad de la información, se caracteriza principalmente por la capacidad actual de acceder y compartir cualquier información instantáneamente desde cualquier parte del mundo.

La evolución de las nuevas tecnologías ha permitido grandes avances, como por ejemplo la enseñanza online, el comercio electrónico, el "teletrabajo" y la comunicación sin fronteras entre usuarios en cualquier punto del mundo.

Sin embargo, también ha dado pie al desarrollo de, en primer lugar, nuevos delitos, llamados "delitos informáticos" que han sido recogidos en la última reforma del Código Penal en el año 2015, no están recogidos de forma ordenada pero sí se encuentran dispersos a lo largo del articulado. Entre ellos destacan: el acceso no autorizado a sistemas informáticos recogido en el artículo 197 bis, los delitos informáticos relacionados con la propiedad intelectual e industrial del artículo 270, los fraudes informáticos recogidos en el artículo 248, entre otros.

En segundo lugar las nuevas tecnologías han facilitado nuevas formas de cometer delitos, se han llegado a convertir en peligrosos instrumentos para la comisión delictiva. Gracias al anonimato que garantizan los nuevos medios telemáticos, la investigación de estos delitos se ha vuelto una tarea de especial complejidad que dio pie, entre otras, a una reforma de la Ley de Enjuiciamiento Criminal en el año 2015.

En este trabajo estudiaremos un nuevo medio de investigación, incluido mediante la Ley Orgánica 13/2015 que modifica la Ley de Enjuiciamiento Criminal, el agente encubierto informático (AEI), regulado en los apartados 6 y 7 del artículo 282 bis.

Previo a este análisis en concreto, es interesante estudiar la tónica general de la LO que hemos mencionado anteriormente, para entender la gran extensión que hoy en día tienen las nuevas tecnologías en la comisión de delitos y, por ello, la necesariedad de las mismas en su investigación.

2. MODIFICACIÓN DE LA LEY DE ENJUICIAMIENTO CRIMINAL. LEY ORGÁNICA 13/2015

La reforma de la LECrim se llevó a cabo mediante 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.

El propio texto de la Ley comienza su preámbulo expresando la necesidad de cambiar determinadas cuestiones de la actual LECrim sin esperar a una reforma de la misma en su totalidad. La falta de desarrollo normativo sobre ciertas cuestiones, tanto sustantivas como procesales, dio lugar a que fueran atendidas de acuerdo a la jurisprudencia. Es decir, han sido los jueces lo que se han encontrado en la posición de ir creando una línea de actuación sobre la materia no recogida por la Ley.

En términos generales, esta reforma intenta definir los límites a los que puede llegar el Estado a la hora de investigar sin llegar a cometer intromisiones en la vida privada de los ciudadanos que puedan llegar a vulnerar cualquiera de sus derechos fundamentales recogidos por la Constitución.

Por tanto, los hitos principales de esta modificación son: por un lado, la adaptación a las exigencias procesales de la Unión Europea; por otro, satisfacer la necesidad de actualizar una Ley aprobada en 1882 a los nuevos tiempos, como indica Manuel Marchena "*la situación de interinidad no permitía a los poderes públicos confiar en el paso del tiempo como fuente generadora de soluciones improvisadas*".[1]

Así, para acabar con esta situación de incertidumbre jurídica y poder garantizar un sistema jurídico de calidad y adaptado a los nuevos tiempos, se promulga la modificación de ciertos aspectos de la Ley de Enjuiciamiento Criminal, con esta norma de rango orgánico.

[1] Marchena Gómez, M., González-Cuéllar Serrano, N. (2015). *La reforma de la Ley de enjuiciamiento criminal en 2015*. Madrid: Ediciones Jurídicas Castillo de Luna. p.199

Antes de la reforma, la LECrim regulaba, como única medida de investigación de esta índole, la interceptación de las comunicaciones postales, telegráficas y telefónicas en el artículo 579. Este tipo de comunicación se conoce que se ha quedado obsoleta; los medios físicos, como forma de comunicación a distancia, han caído en desuso para ser sustituidos por mensajería instantánea (Telegram, Whatsapp…) o redes sociales, mucho más ágiles y populares hoy en día.

En la reforma, el Capítulo IV pasa a detallar de forma más extensa las "*disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos".*

En la nueva redacción de este articulado se desarrollan los supuestos generales que se aplicarán a todas las nuevas medidas de investigación, y que iremos concretando posteriormente, como es el requisito de proporcionalidad, los requisitos para el ámbito de aplicación, la duración de la medida y las características de la autorización.

Con respecto a este último punto es necesario observar que se establece un periodo 3 meses prorrogable hasta 18, un gran avance en la seguridad jurídica del investigado, ya que en la redacción anterior no se encontraba este límite y quedaba la duración de la medida a discrecionalidad del Juez.

El Capítulo V es a partir del cual se van concretando las medidas: comienza con "*la interceptación de las comunicaciones telefónicas y telemáticas*"; y en este caso, se amplía la regulación a los teléfonos móviles, ordenadores portátiles…, es decir, a los nuevos medios telemáticos personales de cualquier clase. Es importante destacar que, dado el gran alcance de información al que se puede acceder en estos dispositivos, se deja en manos del Juez competente delimitar el alcance de la investigación en el caso concreto, para así seguir la línea de protección al ciudadano y proporcionalidad de todo este texto legal.

La regulación respecto a la captación y grabación de comunicaciones orales se encuentra en el Capítulo VI. Hasta la fecha, no estaba regulada en el proceso penal, y se tiene en cuenta ahora porque, en primer lugar, se ha visto que para la resolución de algunos casos, puede llegar a resultar indispensable. Pero sobre todo, porque se estaba aplicando el artículo 579 de la LECrim, mencionado anteriormente, de forma analógica, un precepto insuficiente que no impedía "*obtener de él la máxima elasticidad*".[2]

En este capítulo se detalla que se podrán colocar los dispositivos de grabación en lugares tanto abiertos como cerrados, es decir, en el domicilio del investigado; y además, se podrán complementar, en algunos casos concretos, con la captación de imágenes -regulándolo en el Capítulo VII-. Estas medidas afectan directamente contra el artículo 18.2 de la CE sobre la inviolabilidad del domicilio, y es por ello que en estos casos la autorización judicial, además de todo lo que se le exige en términos generales, deberá detallar el por qué de permitir este acceso y concretar el lugar que se va a vigilar.

El problema principal que ambas medidas plantean es la utilidad real que se puede esperar de ellas. La LECrim establece en el art. 588 quater b) que la medida estará "*vinculada a comunicaciones que puedan tener lugar en uno o varios encuentros concretos del investigado con otras personas y sobre cuya previsibilidad haya indicios puestos de manifiesto por la investigación*".
Es decir, sólo podrán estar los dispositivos de grabación en funcionamiento cuando el encuentro concreto que se quiere recoger se esté produciendo. Como la Ley no prevé que los dispositivos se queden inactivos pero instalados, el coste y la complicación de la instalación de todo el equipo presenta un escollo para la utilización de esta medida que podrá ser solucionado en un futuro cuando, por ejemplo, *"se pueda conseguir una desconexión automática real y total desde la distancia*".[3]

---

[2] Marchena Gómez, M., González-Cuéllar Serrano, N. (2015). *La reforma de la Ley de enjuiciamiento criminal en 2015*. Madrid: Ediciones Jurídicas Castillo de Luna. p. 336
[3] Paloma Conde-Pumpido. Fiscalía Especial Antidroga. *Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos.* 2015

3. SUPUESTO DE HECHO. HECHOS PROBADOS.

Sentencia de la Sala de lo Penal, Sec. 4ª Audiencia Nacional. nº 1519/2018 26 de abril.

El ISIS, con objeto de captar adeptos para establecer el Califato Global, además del contacto directo de sus miembros, se sirve de un sistema de llamamiento global mediante las redes sociales utilizando la excusa de ser un mandato religioso.

El acusado desarrolla, desde el primer trimestre de 2015, a través de las redes sociales -en concreto, Facebook, Google plus o YouTube-, la misión de difusión de la ideología radical yihadista encomendada por DAESH, con objeto de atraer potenciales partidarios en favor de la yihad violenta.

El acusado invitó y admitió entre su grupo de amigos al agente encubierto informático en abril de 2016 y mantuvo algunas conversaciones de temas generales a través de Messenger.

Una vez que surgió cierta confianza entre ambos, a mediados de julio de 2018, pocos días después del atentado de Niza, el acusado aconsejó a su interlocutor que se cuidara “porque había racismo” (se entiende contra los musulmanes). Más adelante, en septiembre de 2016, el agente le comunicó su intención de ir a Turquía, preguntándole si conocía a alguien dispuesto a trasladarse a la zona. El acusado, al contestar, le dijo que no conocía a nadie, le deseó buen viaje y añadió "ojalá pudiera ir yo, pero sabes que tengo familia que mantener y mis padres me necesitan".

El acusado fue detenido y en uno de los ordenadores que le fueron intervenidos figuran 105 búsquedas del Estado Islámico realizadas entre el 31/12/2015 y el 05/03/2016, y otras tantas búsquedas a través de la plataforma YouTube.

En ese mismo dispositivo aparecieron solicitudes de adhesión al DAESH a través del juramento de lealtad al Califato, así como la imagen del globo terráqueo y, sobre él, la bandera del Estado Islámico. Esa misma imagen se encontró como fondo de pantalla de la Tablet Samsung Galaxy del acusado intervenido en el domicilio.

4. EL AGENTE ENCUBIERTO INFORMÁTICO

4.1. DEFINICIÓN

En España, nuestro ordenamiento jurídico no recoge una definición clara de esta nueva figura regulada por la LECrim, es por ello que, recogiendo la Jurisprudencia de nuestro país y basándose en el derecho comparado, algunos autores sí han llegado a una definición precisa del agente encubierto online.

Javier Zaragoza Tejada lo define como "*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 practicas delictivas producidas a través de la misma*".[4]

El AEI está además definido en numerosas sentencias incluso antes de la reforma de la LECrim, se puede observar mediante estos ejemplos la necesidad que había en nuestro ordenamiento de regular esta figura.

Por ejemplo, en la STS 1140/2010, 29 de diciembre se señala que *"El término undercover 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*

[4] Zaragoza Tejada, J. y Bermúdez González, J. (2017). *Investigación tecnológica y derechos fundamentales*. Cizur Menor (Navarra): Aranzadi-Thomson Reuters. p. 329

y permite recabar información sobre su estructura y modus operando, así como obtener pruebas sobre la ejecución de hechos delictivos".

Además de esta definición, hay numerosas sentencias que ya hacían referencia a las actividades del agente encubierto en el ámbito informático, como la STS 767/2007, que establece: "*…lo cierto es que los agentes de la autoridad, cuando realizan las labores habituales de vigilancia para prevenir la delincuencia informática… realizaron las investigaciones oportunas, y, sólo cuando tuvieron la convicción de estar efectivamente en presencia de hechos presuntamente delictivos, confeccionaron el oportuno atestado que remitieron a la Fiscalía de la Audiencia Provincial… Tal método de proceder es absolutamente correcto y ninguna objeción puede merecer".* [5]

Así, en el año 2015 se incluyen los apartados 6 y 7 del art. 282 bis, que establecen que esta nueva figura deberá tratarse siempre de un miembro de la Policía Judicial; y además, señalan una de las principales diferencias con el agente encubierto tradicional, que deberá estar autorizado únicamente por el Juez de Instrucción y no por el Ministerio Fiscal, como se da en el caso anterior.

Esta diferenciación con el agente encubierto tradicional es importante, ya que en el curso de las investigaciones que se llevan a cabo por el AEI se pueden ver afectados derechos fundamentales como el derecho a la intimidad, a la inviolabilidad del domicilio o al secreto de las comunicaciones entre otros.

[5] Sentencia del Tribunal Supremo 767/2007 del 3 de octubre.

4.2. ÁMBITO DE ACTUACIÓN

El artículo 282 de la LECrim, en el apartado 6, nos delimita el ámbito de actuación del agente encubierto informático a aquellos delitos que "*se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a".*

Es decir, esta medida de investigación tiene cabida en todas aquellas de actividades que se puedan considerar como actividades propias de delincuencia organizada, que se encuentran definidas y enumeradas *numerus clausus* en la propia ley.

Además de los mencionados anteriormente, y por la remisión que la propia LECrim hace al artículo 579.1, se amplía el ámbito de actuación de esta medida a los delitos cometidos *"a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación".*

Sin lugar a dudas, esta modificación amplía el ámbito de actuación del AEI, pero con respecto al requisito de delincuencia organizada, da lugar a que no se puedan investigar por estos medios muchos delitos que se cometen hoy en día en , pero que no cumplen los requisitos establecidos para considerarse actividades realizadas por una organización criminal, o no están contenidos en el listado del artículo 282 bis 4 de la LECrim. [6]

---

[6] *a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.*

b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.

c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.

d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal.

e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.

f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal.

g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal.

h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal.

Esta situación se puede dar en el caso de delitos como: la pornografía infantil, el hacking, las estafas masivas, o incluso la captación para actividades derivadas del terrorismo islámico, cuando no se lleva a cabo de manera coordinada sino de forma individual.

Así, por un lado, al no haber jurisprudencia clara sobre este asunto, se podría argumentar que la legislación, al acotar los delitos para cuya investigación se puede hacer uso del AEI, no cumple completamente su función de frenar todos los delitos que se comenten a través de Internet o de las redes en general.

Pero, por otro lado, es importante tener en cuenta que esta medida de investigación debe ser usada con cautela, en todo caso, dada la importancia de los bienes jurídicos en juego. El *ciberpatrullaje,* por ejemplo, que es la actividad de investigación que algunos agentes realizan en Internet con la finalidad de prevenir delitos, no presentaría ningún problema si se realizara en canales abiertos de comunicación.

Sin embargo, si hay indicios de comisión delictiva será imprescindible contar con la autorización judicial correspondiente a la hora de realizar la investigación para que la prueba tenga en el momento del juicio, plena validez; pero sobre todo, para garantizar que se respetan los derechos fundamentales del investigado.

---

i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal.

j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal.

k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.

l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.

m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal.

n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal.

o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando.

4.3. CANALES DE COMUNICACIÓN CERRADOS

Otro de los puntos sobre los que hacer hincapié con respecto a esta nueva reforma de la LECrim es determinar el campo de actuación del AEI, es decir, determinar cuáles son los canales de comunicación cerrados para los cuales es necesaria la autorización judicial para investigar; ya que, aplicando *sensu contrario* la legislación, para aquellos canales de comunicación que permanezcan abiertos, no hará falta hacer uso de esta figura.

La jurisprudencia ha reiterado, con respecto a este tema, que "*no se precisa de autorización judicial para conseguir lo que es público; de manera que las actividades públicas realizadas en Internet, susceptibles de ser conocidas por tanto también por la policía, no se hallan protegidas por el art. 18.1 ni por el 18.3 de la Constitución".*[7]

La propia Exposición de Motivos de la Ley 13/2015 señala "*(…) Se regula la figura del agente encubierto informático que requiere autorización judicial para actuar en canales cerrados de comunicación (puesto que en los canales abiertos, por su propia naturaleza, no es necesaria) y que a su vez, requerirá una autorización especial (sea en la misma resolución judicial, con motivación separada y suficiente, sea en otra distinta) para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación*." De esto se puede deducir que con la modificación de la LECrim la intención del legislador es la no utilización del AEI en aquellos foros abiertos de comunicación en los que su actuación se estaría extralimitando.

La controversia se haya, sin embargo, en determinar cuándo se considera que en los medios telemáticos las informaciones son públicas o privadas.

En este ámbito no hay un desarrollo jurisprudencial concreto, pero siguiendo la línea de la lógica, se podría establecer que, a pesar de tener que dar de alta un perfil

[7] Roberto Valverde Megías "*Cuestiones procesales relativas a la investigación de los delitos en red*". 2015.p. 20

personal de forma obligatoria para acceder a todas las redes sociales en las que se comparte contenido personal (ej. Facebook, Twitter, Instagram, foros de opinión…), una vez dentro, todo aquello que no haya sido privatizado por el usuario que lo publica, está al alcance de los demás usuarios de la red en cuestión, es decir, serían considerados públicos, a no ser que para acceder a ellos el usuario tuviese que dar una expresa autorización a otra persona, en concreto, para poder proceder a su visualización. En este caso entonces, sí estaríamos ante canales de comunicación cerrados en medios telemáticos.

5. ACTUACIONES DEL AGENTE ENCUBIERTO INFORMÁTICO

La exposición de motivos de la Ley Orgánica 13/2015, que como ya se ha indicado anteriormente reforma la Ley de Enjuiciamiento Criminal, recoge una regulación muy actualizada sobre los medios de investigación tecnológica, que eran muy necesarios para poder poner fin a las nuevas formas de "ciberdelincuencia".

Entre otras medidas la LECrim ahora regula la interceptación de comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de medios electrónicos, la utilización de dispositivos técnicos de captación de imagen, de seguimiento y de localización, el registro de dispositivos de almacenamiento masivo de información, etc.

El agente encubierto informático es otra de las novedades que se incluye, y es preciso analizar cuáles son las actuaciones que tiene "permitidas" para actuar, en todo caso, acorde a lo dispuesto en la LECrim.

El segundo párrafo del art. 282 bis 6 de la LECrim establece que el agente encubierto "*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*".

Mediante este artículo la LECrim nos remite al artículo 588 ter a, sobre los presupuestos de autorización para la interceptación de comunicaciones telefónicas y telemáticas. Es un sistema *numerus apertus* que implica que esta técnica de investigación concreta será libremente designada por el Juez, cuando sea necesario, pero siempre que verse sobre los delitos del art. 579.1 de esta misma Ley que son:

"*1º. Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.*

2º. Delitos cometidos en el seno de un grupo u organización criminal.

3º. Delitos de terrorismo".

Por otro lado, el apartado 7 del artículo 282 bis de la LECrim establece que siempre que haya medida autorización del Juez, será posible 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".*

A modo de síntesis y para concretar, podemos establecer un listado de las actuaciones concretas de investigación que puede llevar a cabo un agente encubierto informático y que están recogidas en el Capítulo IV de la exposición de motivos de la Ley Orgánica 13/2015.

- Realizar imágenes o grabar conversaciones privadas que hayan sido mantenidas con el sujeto investigado.
- Enviar cualquier tipo de archivo que por su contenido pueda ser considerado ilícito.
- Analizar los algoritmos que han sido utilizados para la obtención y posterior identificación de los archivos.

Javier Zaragoza Tejada en sus comentarios sobre esta figura resalta un tema importante con respecto a los archivos ilícitos que son puestos en conocimiento del Tribunal. No hay ninguna regulación al respecto de qué pasa después con dicho material, y sería necesario aclarar que debería ser "*recuperado íntegramente, tanto por los intereses de las partes implicadas como por el peligro que supone que sea indebidamente difundido".* [8]

[8] Zaragoza Tejada, J. y Bermúdez González, J. (2017). *Investigación tecnológica y derechos fundamentales*. Cizur Menor (Navarra): Aranzadi-Thomson Reuters. p.350

6. DELITO PROVOCADO Y AGENTE PROVOCADOR

La actividad del agente encubierto informático, como ya se ha indicado anteriormente, se engloba dentro de las diligencias de investigación: éstas están destinadas a descubrir todo aquello que tenga que ver con el hecho punible, o con la persona sospechosa en el caso concreto.

Desde un primer momento, la medida se basa esencialmente en recabar información a través de canales cerrados de comunicación y mediante una identidad fingida. Así, el agente encubierto se vale de un anonimato previamente autorizado para recabar información que no ha podido ser obtenida por otra vía.

Esta situación establece una problemática que ha sido ampliamente estudiada y sobre la que se ha dictado un gran número de sentencias en España. Concretamente, hacemos referencia al conflicto que surge frente a la posibilidad de que el propio agente sea, por su actuación, provocador del delito que está investigando.

El agente provocador no está regulado en nuestro ordenamiento jurídico; sin embargo, al haber jurisprudencia sobre el tema, se puede llegar a una definición bastante acertada, como es la de Perals Calleja: "*el denominado impropiamente agente provocador se asemeja a la figura del agente encubierto en que se trata de un funcionario policial que se acerca a una organización o un grupo de delincuentes o, incluso, a uno aislado, escondiendo su condición de funcionario público y finge intervenir en el delito y de esta manera 'provoca' la consumación del mismo. Se distingue claramente de la figura prevista en el art. 282 bis de la LECrim porque en este caso no se precisa la obtención de una identidad ficticia ni se opera con la previa autorización judicial".* [9]

[9] Perals Calleja, J., *Técnicas de investigación del crimen organizado: el agente encubierto, confidente, regulación en España, validez de la prueba obtenida en el extranjero, problemas prácticos de la heterogénea regulación de la materia,* Cuadernos Digitales de Formación, 2010.

De igual modo, la STS 1166/2009 de 19 noviembre trata sobre el delito provocado y afirma: *"la provocación delictiva es una inducción engañosa, es decir, supone injertar en otra persona el dolo de delinquir, y cuando esto se hace con la colaboración policial, se produce el efecto perverso de que la policía lejos de prevenir el delito, instiga a su comisión —elemento subjetivo— bien que sin poner en riesgo ningún bien jurídico, pues en la medida que lo apetecido es la detención del provocado —elemento objetivo—, toda la operación está bajo el control policial por lo que no hay tipicidad ni culpabilidad, ya que los agentes de la autoridad tienen un control absoluto sobre los hechos y sus eventuales consecuencias —elemento material—, siendo estos tres elementos los que vertebran y arman la construcción del delito provocado*".

En este caso, se habla de una figura que no está protegida por el ordenamiento jurídico, ya que es causante del propio delito y está fuera de las facultades que la propia LECrim otorga a los agentes policiales, que están recogidas en los art. 282 y ss. de esta Ley, y que básicamente se centran en la propia "*averiguación del delito y descubrimiento del delincuente".*[10]

La Sentencia del Tribunal Supremo 690/2010, del 1 de julio trata sobre el concepto de delito provocado para desarrollar la acción inductora del agente provocador y lo expone del siguiente modo: "*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".*

[10] Gimeno Sendra, V. y Díaz Martínez, M. (2018). *Manual de derecho procesal penal*. Madrid: COLEX.P. 354.

Sensu contrario se entiende que en aquellos casos en los que sí había actividad previa a la comisión del delito, no se puede hablar de agente provocador, ni por lo tanto de delito provocado, ya que se entiende que el funcionario policial "*intenta esclarecer delitos ya cometidos y, en última instancia, poner término a una actividad delictiva que se está cometiendo*".[11]

En definitiva, para poder establecer que efectivamente la causa del delito es la actuación de agente provocador, uno de los principales indicadores es la existencia o no de actividad criminal previa, o lo que es lo mismo, que no haya ningún tipo de actuación inductora a delinquir sobre alguien que por su libre decisión no iba a llevar a cabo actuaciones constitutivas de delito.

Esta doctrina está muy consolidada en la Sala Segunda del Tribunal Supremo, siempre que la actuación del agente de lugar a que una persona que no tenía intención de cometer actividades delictivas finalmente, dada la incitación del agente, cometa un delito, la actividad policial en este caso es *"completamente contraria a la Ley y por lo tanto inadmisible por nuestro ordenamiento jurídico".* [12]

La Sentencia de la Sala de lo Penal de la Audiencia Nacional 1519/2018 del 26 de abril, cuyos hechos probados se han resumido al comienzo de este análisis, lleva a cabo, en el primero de sus fundamentos de derecho, un análisis sobre las peticiones de nulidad alegadas por la defensa.

En este caso, la defensa pide la nulidad de *"la autorización de las diligencias llevadas a cabo por el agente encubierto, entendiendo que ha llevado a cabo la labor de un agente provocador*''. [13] Entre las cuestiones que aborda el Tribunal a la hora de pronunciarse sobre la actuación de fondo del agente encubierto hace referencia a la inexistencia de delito provocado.

La defensa cuestiona que el agente, en su labor de investigación ha sobrepasado el limite de las actuaciones que le había marcado el Juez de Instrucción en la autorización

[11] Gimeno Sendra, V. y Díaz Martínez, M. (2018). Manual de derecho procesal penal. Madrid: COLEX. Pág. 354.
[12] STS 360/2016, del 10 de febrero y STS 571/2008, del 25 de septiembre.
[13] Sentencia de la Sala de lo Penal de la Audiencia Nacional 1519/2018 26 de abril.

previa y así ha llegado a convertirse en un agente provocador. El Tribunal expone que en ningún caso el agente ha llevado a cabo alguna actuación que haya dado lugar a la comisión del delito objeto del caso, fundamenta esta postura en que, ni desde un punto de vista teórico, ni desde un punto de vista operativo, el agente ha vulnerado los principios legales a los que sus labores de investigación están atadas.

Concretamente, el Tribunal, al hablar desde un punto de vista teórico sobre la supuesta existencia de agente provocador planteada por la defensa, alega refiriéndose a diversas Sentencias del Tribunal Supremo que sólo se da cuando "*guiado por la intención de detener a los sospechosos o de facilitar su detención, provoca a través de su 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".*[14]

No es ésta la situación que se da en el caso porque no surge en el agente, como sería necesario para hablar de agente provocador, todo el *"iter criminis*" o camino del delito. Éste se compone no sólo de la inducción a delinquir, sino que se da *"desde la fase de ideación o deliberación a la de ejecución, como consecuencia de la iniciativa y comportamiento del provocador".*[15]

Así, en esos casos, la causa de la actividad criminal estará desde un primer momento viciada por la actividad del agente, situación que en el caso expuesto no se contempla.

En primer lugar, porque la autorización a la investigación del agente se otorgó cuando ya se habían agotado las demás vías de investigación y la Brigada Provincial de Investigación de la Jefatura Superior de Policía de Asturias solicitó esta medida de investigación ante la "p*resunta existencia de un delito de colaboración o pertenencia a organización terrorista, sirviéndose para tal fin de las redes sociales*"[16]; por lo tanto, ya se presumía la existencia del actividad delictiva por parte del acusado.

Además, como explica también la sentencia analizada, en todo caso, el agente cumplió con los requerimientos del Juzgado sobre la puesta en conocimiento de la información.

[14] Sentencia del Tribunal Supremo, Sala Segunda 848/2003 del 13 de junio.
[15] Sentencia del Tribunal Supremo, Sala Segunda 1992/1993 del 15 de septiembre.
[16] Sentencia de la Sala de lo Penal de la Audiencia Nacional 1519/2018 26 de abril.

Por otro lado, la Sala de lo Penal de la Audiencia Nacional también argumenta la inexistencia de agente provocador desde un punto de vista operativo o funcional, es decir, remitiéndose a los actos concretos realizados por el agente durante toda su labor de investigación.

Este aspecto se sustenta claramente en las interacciones que efectivamente tuvo el agente con el investigado. El Tribunal, se basa en primer lugar en que el permiso para acceder a sus redes sociales fue concedido por el acusado, así como una vez ya dentro le permitió visualizar las imágenes, capturas y mensajes que sirvieron de base para esclarecer los hecho y afirmar finalmente en el fallo que el investigado cometió un delito de colaboración en organización terrorista.

Exactamente, y para que no haya lugar a dudas, el Tribunal detalla "*tampoco fue el agente quien tomó la iniciativa enviando una solicitud de amistad al acusado, sino que como aquél relató, fue el acusado quien tomó la iniciativa invitándole a compartir y conocer no sólo sus ideas en favor de la yihad violenta, sino su actividad distribuidora captando la atención de partidarios del Islam radical*".[17]

A través de este análisis detallado de los hechos y las interacciones entre agente e investigado el , hace constar que la labor de control que requiere esta medida de investigación sí se ha llevado a cabo para evitar que, en cualquier momento, las actuaciones del agente pudieran dar lugar a un delito provocado.

[17] Sentencia de la Sala de lo Penal de la Audiencia Nacional 1519/2018 26 de abril.

7. MEDIDA RESTRICTIVA DE DERECHOS FUNDAMENTALES

En el desarrollo de este planteamiento se puede considerar que se está dando por válido el uso del engaño a través de los medios telemáticos para proceder a una invasión de la intimidad y de la privacidad de los ciudadanos.

En primer lugar, hay que reiterar en la idea ya expuesta anteriormente, de la obligatoriedad de una autorización por parte del Juez de Instrucción, y no por el Ministerio Fiscal. Es importante ya que representa una garantía para los ciudadanos frente a la posible vulneración de derechos fundamentales, como puede ser el derecho al secreto de las comunicaciones, entre otros previamente mencionados. Es decir, se trata de otorgar a los ciudadanos de protección frente a la "invasión" de los poderes públicos en este caso.

Englobando todos los derechos fundamentales que ya hemos mencionado, existe, por desarrollo jurisprudencial, un derecho fundamental nuevo que se deriva de la proliferación y normalización del uso de las nuevas tecnologías en todos los ámbitos de la vida de los ciudadanos -ya que actualmente tanto en la vida personal como laboral tienen una gran presencia los medios telemáticos-. Son forma de ocio, de almacenamiento de la información, medio y método de trabajo y de organización, y de planificación en la vida cotidiana de la mayoría de las personas actualmente.

Es por todo esto que se puede hablar de "*derecho a la identidad virtual*"[18]. Este concepto nace en la Sentencia del Tribunal Constitucional 173/2011 de 7 de noviembre, en la que el Tribunal considera que en un ordenador, las personas almacenan un conjunto de datos que individualmente analizadas no suponen una violación expresa de los derechos fundamentales, pero que al hacerlo en su conjunto "*no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o*

[18] Zaragoza Tejada, J. y Bermúdez González, J. (2017). *Investigación tecnológica y derechos fundamentales*. Cizur Menor (Navarra): Aranzadi-Thomson Reuters. Página 5.

individualidad de la persona".[19]

El Tribunal Supremo también ha desarrollado este criterio, por ejemplo en la Sentencia de la Sala Segunda 342/2013, del 17 de abril. En ella se refiere al artículo 18.4 de la CE que expone que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos" y sigue desarrollando el derecho al propio entorno virtual para hacer hincapié en la necesaria cautela que han de tener los poderes públicos, en este caso que nos ocupa, el Juez de Instrucción a la hora de permitir la intromisión en la esfera más personal de los ciudadanos.

Además, establece la necesidad de razonamiento exhaustivo que ha de llevar consigo la autorización puesto que estas actuaciones conllevan, en cualquiera de los casos, una vulneración de los derechos más protegidos y a la vez elementales que se han de garantizar para todos en el uso de las nuevas tecnologías.

7.1. PRINCIPIO DE PROPORCIONALIDAD

Es importante en este análisis hacer referencia al estudio que se ha de llevar a cabo sobre el principio de proporcionalidad a la hora de hacer uso de esta medida.

La finalidad del estudio de este criterio está en la colisión que se da entre la protección y el respeto de los de los derechos fundamentales de lo ciudadanos, y el deber del Estado de Derecho de proteger el orden social.

La propia LECrim establece en su artículo 588 bis a) que "*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 principio de proporcionalidad no está desarrollado como tal en ninguna ley de nuestro ordenamiento jurídico, es herencia de la doctrina del Tribunal Constitucional alemán y su creación en nuestro país es puramente jurisprudencial.

[19] Sentencia del Tribunal Constitucional 173/2011 de 7 de noviembre.

Se podría definir como aquel criterio que mediante unos presupuestos y requisitos establecidos sirve para limitar el uso de medidas restrictivas de derechos humanos y garantiza así que no se produzcan injusticias, se garantice el bien común y se protejan los derechos y libertades de los ciudadanos.

A continuación procederemos a un análisis de los elementos que definen el principio de proporcionalidad refiriéndolo a la autorización que el Juez de Instrucción otorgará para el uso del agente encubierto informático, considerado como medida de investigación restrictiva de derechos fundamentales.

En primer lugar, los presupuestos que ha de cumplir el principio de proporcionalidad son:

A) Presupuesto de legalidad.

Se trata de un presupuesto formal que establece que la medida debe estar contemplada en la Ley, en este caso, como ya hemos expuesto, su regulación se encuentra en el art. 282 bis de la LECrim.

B) Presupuesto de justificación teleológica.

Se define como aquel presupuesto material que "*exige que la limitación de los derechos fundamentales se verifique por causa de finalidades constitucionalmente legítimas*".[20]

El uso de esta medida está dirigido a la investigación de un listado *numerus clausus* de delitos considerados graves por el Código Penal, es decir, aquellos que conlleven una pena grave, superior a 5 años. Al dedicarse el uso de esta figura a la investigación de delitos concretos y graves podemos establecer, sin lugar a dudas, que se trata de la persecución de un "*fin constitucionalmente legitimo y socialmente relevante*"[21]

[20] González-Cuéllar Serrano. (1990). *Proporcionalidad y derechos fundamentales en el proceso penal*, Madrid. Ed. Colex . p. 101-104

[21] Banacloche Palao, J. y Zarzalejos Nieto, J. (2018). *Aspectos fundamentales de derecho procesal penal*. 4ª ed. Madrid: Wolkers Kluwer. P. 68

Además del concepto de gravedad del delito, se puede establecer que todas aquellas nuevas formas de perpetración de delitos debido al uso de las nuevas tecnologías requieren de nuevas formas de investigación. Por ello, la justificación teleológica también se podría encontrar en el hecho de hacer uso de todas las medidas posibles para impedir la impunidad de delitos que no se han conseguido descubrir siguiendo los métodos de investigación tradicionales.

La Sentencia del Tribunal Constitucional 207/1996, de 16 de diciembre fue la primera en desarrollar en España el concepto de principio de proporcionalidad y desarrolló los tres requisitos o condiciones para que se cumpla de la siguiente manera:

A) Idoneidad: "*Si la medida es susceptible de conseguir el objetivo propuesto*".[22]

Para el análisis de la figura que nos ocupa, este requisito pretende evitar que se use para investigar delitos que sean poco lesivos o que no supongan un prejuicio relevante para la sociedad, ya que éste no es el "objetivo propuesto".

b) Necesidad: "*Si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia*".[23]

C) Proporcionalidad en sentido estricto: "*Si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto*".[24]

El análisis de estos últimos dos requisitos se puede llevar a cabo simultáneamente ya que la LECrim, en el art. 282 bis, establece que los juicios de proporcionalidad y necesariedad se harán en base a la finalidad de la investigación.

Es decir, la autorización del Juez que da pie a la infiltración se hace en un primer momento en base a indicios o presunciones de existencia de una conducta posiblemente constitutiva de delito o de la presencia de una organización criminal. Así, la finalidad perseguida debe ser necesaria y proporcional a la medida tomada.

[12, 13, 14] Sentencia del Tribunal Constitucional 207/1996, de 16 de diciembre. BOE núm. 19, de 22 de diciembre de 1997.

7.2. OTRAS OBSERVACIONES SOBRE LA RESOLUCIÓN JUDICIAL PARA AUTORIZAR LA ACTUACIÓN DEL AGENTE ENCUBIERTO.

En la Sentencia de la Sala de lo Penal de la Audiencia Nacional 3462/2018 del 25 de septiembre, podemos encontrar un ejemplo del Auto de autorización del Juez de Instrucción en el que permite el uso del agente infiltrado para la investigación de un supuesto delito de captación y adoctrinamiento terrorista.

En dicho auto se establecen una serie de medidas de control de la actuación del AEI que están recogidas en la LECrim y que podemos entender que también están dirigidas a la protección de los derechos fundamentales de los investigados, es decir, se lleva a cabo una exhaustiva labor de vigilancia del cumplimiento de las actuaciones por parte del Juez para garantizar la proporcionalidad de la medida aplicada.

En primer lugar, en el Auto se recoge la necesidad de informar al agente encubierto personalmente de sus obligaciones, exigencias y actuaciones habilitadas, así como las situaciones sociales y jurídicas en las que está autorizado a utilizar la identidad supuesta que le fuera otorgada.

Por ejemplo, establece concretamente las redes sociales en las que el AEI se deberá dar de alta con un gran nivel de detalle "*Facebook, Twiter, Google +, Badoo, Whatsapp, Telegram, Line, Skype, Snapchat, Neverline, Viber y mnbr.info*".[25] Y una vez hecho, remitir un Acta al Juzgado de Instrucción que corresponda y que contenga la creación de los perfiles autorizados.

Además, se establece el plazo durante el cual podrá actuar el agente encubierto informático, en este caso concreto, 6 meses. La exposición de motivos de la LO, en su apartado IV, establece: "*plazo de tres meses como duración máxima inicial de la intervención, plazo que es 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 motivaron aquella*".

[25] Sentencia Sección 3ª de la Sala de lo Penal de la Audiencia Nacional 3462/2018 del 25 de Septiembre.

Por otro lado, se recogerá en la autorización, siempre, el deber de información que exige la LECrim en el artículo 282 bis 1 -"*la información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación*"-.

No se establece en la LECrim la periodicidad concreta con la que el AEI deberá entregar la información; se entiende que queda en manos del Juez de Instrucción competente concretarlo en cada caso, siempre atendiendo a las circunstancias concretas, ya que en ocasiones puede ser incluso dañino para la investigación que el agente se desvincule de su tarea o incluso puede llegar a ser peligroso para él mismo.

En el caso de este Auto, el Juez especifica que la información que vaya recabando deberá ser remitida, en todo caso, mensualmente; y toda ella tendrá que constar en una pieza separada y secreta.

Siguiendo con lo establecido en la Exposición de Motivos de la LO 13/2015 y en la línea de análisis que estamos llevando de evitar que haya una intromisión excesiva y/o lesiva en los derechos fundamentales del investigado, se controlarán todos los documentos y soportes utilizando un "sistema de sellado", una firma electrónica que corrobore la entrega íntegra de lo descubierto y su autenticidad.

En el caso expuesto al comienzo del trabajo, se usa el agente encubierto como medida de investigación, la autorización obligatoria del Juez de Instrucción llega de la siguiente manera:

En primer lugar, como ya hemos indicado anteriormente, la Brigada Provincial de Investigación de la Jefatura Superior de Policía de Asturias propone la autorización de un agente de la Policía Judicial "*adscrito a la propia unidad- que resultó ser el secretario de la misma- para actuar con identidad supuesta en el ámbito de las comunicaciones telemáticas con el investigado*".[26]

Tras darle traslado al Ministerio Fiscal, que se mostró favorable, el Juez de Instrucción del caso abrió una pieza separada en la que, a través de un Auto de 12 folios, autoriza

[26] Sentencia de la Sala de lo Penal de la Audiencia Nacional 1519/2018 26 de abril.

el contacto con el investigado a través de redes sociales durante un mes, prorrogable si fuera necesario, y con todas las condiciones de actuación del mismo que se detallan a continuación:

"1º.- Autorizar al funcionario habilitado para poder intercambiar, en el periodo habilitado, intercambiar y enviar por sí mismo archivos ilícitos por razón de su contenido; 2º.- Mantener secreta en pieza separada que quedará en poder del Letrado de la Administración de Justicia la resolución habilitante; 3º.- Grabar íntegramente las conversaciones en el soporte correspondiente que se remitirá al juzgado donde constarán las grabaciones e imágenes con las transcripciones de interés. 4º.- En el caso de que la investigación pueda afectar a los derechos fundamentales, el agente deberá solicitar del organismo judicial competente las autorizaciones que establezcan la Constitución y la ley. 5º.- 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 6º.- 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 ".[27]

Mediante este Auto tan detallado, el Juez de Instrucción cumple con la exhaustividad requerida para el uso de esta medida de investigación, explicando no sólo las razones por las que es necesaria, sino también dejando constancia de las actas levantadas y de la entrega al letrado defensor de todos los tomos con la documentación recopilada.

[27] Sentencia de la Sala de lo Penal de la Audiencia Nacional 1519/2018 26 de abril.

8. RESPONSABILIDAD DEL AGENTE ENCUBIERTO

El deber de información al que hemos hecho referencia anteriormente para la salvaguarda de los derechos fundamentales, está contenido en la LECrim en el art. 282 bis 5. En este artículo la Ley también establece la exención de responsabilidad criminal para el agente encubierto.

Es importante en este punto destacar que el análisis de la responsabilidad penal del agente encubierto no hace referencia específicamente al agente encubierto informático, sino que está prevista para la figura tradicional y tras la modificación de la Ley de Enjuiciamiento Criminal se extiende al AEI.

Así, la LECrim en el artículo antes mencionado establece que no habrá responsabilidad criminal derivada de las actuaciones del agente encubierto informático cuando actúe con la debida proporcionalidad y no provoque el delito.

Anteriormente, ya hemos hecho referencia a estas dos condiciones; sin embargo, tras la LO 13/2015, no se han llegado a esclarecer algunas cuestiones controvertidas más concretas que sí tienen vinculación directa con las acciones que realiza el AEI.

Se trata de actuaciones que, en algún momento del desarrollo de la investigación, el agente pueda tener que realizar para poder concluirla con éxito, pero que no están completamente reguladas y pueden dar lugar, por ejemplo, a que en el momento del juicio, la defensa intente desestimar lo descubierto como prueba en el caso. Es el caso del envío de archivos ilícitos y el contacto con la organización previo a la autorización del Juez.

En primer lugar, con respecto al envío de archivos ilícitos, la LECrim no enumera los casos en los que el AEI tiene "permitido" cometer un acto ilícito; es por ello que el análisis será posterior a la realización del hecho.

Un ejemplo problemático es la situación no regulada frente a la que se pueden encontrar los agentes en algún punto del ejercicio de su función: el envío de material pornográfico infantil para acceder a ciertos foros que se quieren investigar porque se están cometiendo delitos… ¿Hasta qué punto debería el agente enviar dicho material?

Por un lado es ilícito y viola un bien jurídico protegido pero a la vez será necesario para poder evitar que la comisión delictiva continúe.

Esto conlleva una fuerte inseguridad jurídica para el agente, situación que se salvará si se cuenta con la debida autorización judicial, lo que no significa en ningún caso que la autorización sea una ocasión para desarrollar cualquier tipo de actividad, siempre tendrá que estar bajo las limitaciones del art. 282 bis 5 que se han mencionado a lo largo del trabajo.

Por otro lado, existe el problema del material probatorio obtenido por el agente antes de que haya sido otorgada la autorización que permite comenzar las investigaciones.

En este caso, es importante tener en cuenta que la medida debe cumplir el requisito de necesidad que ya hemos desarrollado anteriormente, es decir, que se use en aquellos casos en los que esté justificada su proporcionalidad, y para ello, ha de ser la menos gravosa para el investigado.

Con este planteamiento llegamos a la situación previa a autorizar la investigación; en todo caso, habrá que verificar que efectivamente existe una organización criminal cometiendo actividades delictivas, pero además es necesario que exista un contacto con aquellas personas que posteriormente van a dar acceso al agente. Es impensable que sin que haya un contacto previo el AEI vaya a poder acceder a las comunicaciones, redes sociales, etc. objeto de la investigación.

Durante este primer periodo de toma de contacto, el agente puede verse ante la tesitura de ser testigo de conversaciones y actividades que posteriormente podrían ser usadas como prueba en el juicio, si finalmente llega a ese término. Es por ello que hay que hacer hincapié sobre la validez de todo ese material cuando el agente era aún "no encubierto".

Al no haber legislación concreta sobre el tema, hay que acudir a la jurisprudencia para poder resolver la cuestión. La STS 655/2007 del 25 de junio, pese a ser anterior a la reforma de la LECrim, dice claramente: "*el que un funcionario policial lleve a cabo tareas de investigación antes de llegar a tener el carácter que regula el art. 282 bis no*

implica que no pueda servir válidamente como testigo respecto a lo visto y oído en tiempo anterior". [28]

Siguiendo el análisis de esta sentencia, se puede entender la lógica que explica que el tratamiento de lo descubierto no será el mismo, ya que entonces se desvirtuaría la importancia de la autorización y es posible que entonces sí se violara el respeto a los derechos fundamentales. Así, en estos casos, sus actuaciones no estarán bajo el amparo de no responsabilidad que brinda el art. 282 de la LECrim.

Para finalizar este análisis es necesario añadir que el Convenio Europeo de Asistencia Judicial en materia penal de 29 de mayo de 2000 , en su artículo 15 hace referencia a la responsabilidad penal de los agentes de las Fuerzas y Cuerpos de Seguridad del Estado y establece que los criterios aplicables a los agentes extranjeros serán aquellos que se apliquen en "*el país donde se esté realizando la operación*".[29]

[28] Sentencia 655/2007 de 25 de junio. Sala de lo Penal. Audiencia Nacional. Sección 1ª, Caso GRAPO

[29] Convenio Europeo de Asistencia Judicial en materia penal de 29 de mayo de 2000
"*Artículo 15. Responsabilidad penal en relación con los funcionarios:*
Durante las operaciones contempladas en los artículos 12, 13 y 14, los funcionarios procedentes de un Estado miembro que no sea el Estado miembro en el que se desarrolla la operación se asimilarán a los funcionarios de este último Estado miembro en lo relativo a las infracciones que pudieran sufrir o cometer."

9. CONCLUSIONES

Tras el análisis en profundidad de los fundamentos de derecho que soportan esta nueva figura jurídica podemos concluir que el agente encubierto informático es una medida cuya incorporación a nuestro ordenamiento jurídico estaba resultando imprescindible, y que su desarrollo contribuye a que la Ley cumpla su objetivo de ir creando un ciberespacio seguro.

De acuerdo a los antecedentes de hecho que observábamos al comienzo del trabajo, y tras todo el desarrollo que se ha llevado a cabo, cabe concluir que, en el caso concreto, el uso de esta medida de investigación cumple con todos los presupuestos legales exigidos.

Como hemos analizado a lo largo del trabajo, la autorización por parte del Juez de Instrucción del caso cumple con los requisitos de exhaustividad que requiere esta medida de investigación, se respeta los principios de proporcionalidad y necesariedad, garantizando así el respeto a los derechos fundamentales del investigado.

Por último, se lleva a cabo un control exhaustivo de todas las actuaciones realizadas, mediante la obligación de entrega de documentos y el deber de informar con periodicidad, en este caso únicamente durante un mes, al Juez competente.

El estudio detallado de las actividades que realiza el agente informático me lleva a la conclusión de que todas ellas, preventivas y defensivas, contempladas en la LECrim garantizan que los delitos cometidos a través de medios telemáticos no puedan escudarse en una impunidad ficticia amparada en la falta de desarrollo normativo.

Es interesante añadir, con respecto al ámbito de aplicación de esta medida, que a pesar del gran avance llevado a cabo tras la reforma de la LECrim, considero que el uso del agente encubierto informático debería extenderse a todos los delitos cometidos en Internet, siempre que el juez competente considere oportuno su uso y sin olvidar los criterios de proporcionalidad y necesariedad que son la base de la actuación del AEI.

Esto no implica que se convierta en una medida de investigación "cotidiana" usada sin ponderar su necesariedad o sin exigir la debida conexión entre el investigado y aquellas vías de investigación que se vayan a explorar, ya que ni por los medios ni por los recursos que conlleva sería posible semejante extensión.

Sin embargo, considero que sí sería necesario seguir avanzando con el desarrollo de esta medida para evitar que en algunas circunstancias la propia LECrim, mediante la enumeración *numerus clausus* de las posibilidades de usar esta figura, pueda dar lugar a que no se pongan todos los medios posibles al servicio de la justicia y de la seguridad de los ciudadanos.

A lo largo de los últimos años, y según va avanzando la tecnología, todos aquellos que quieran escudarse en Internet para seguir llevando a cabo comportamientos delictivos, es muy posible que encuentren la manera, principalmente porque el desarrollo de las nuevas tecnologías es más ágil que el desarrollo normativo. Por eso, es importante que nuestro ordenamiento jurídico garantice, en cualquiera de los casos, la eficacia de la investigación del delito y la nula impunidad del delincuente.

Siguiendo la línea de claridad normativa que el tema requiere, cabe resaltar la inseguridad jurídica a la que se enfrentan los agentes de la Policía Judicial al llevar a cabo estas investigaciones. Las actuaciones que pueden realizar bajo el amparo de la LECrim están contenidas de una manera muy genérica, para evitar conflictos derivados de la discrecionalidad del Juez, en un tema tan delicado y sensible como es la infiltración en organización criminal, el uso de identidad supuesta, el envío de archivos ilícitos y otras muchas acciones que ya hemos indicado durante el trabajo; es importante la labor del legislador de redactar el texto de forma concreta que no dé ningún lugar a dudas y que ayude a garantizar una investigación de calidad.

10. BIBLIOGRAFIA

MONOGRAFÍAS

Banacloche Palao, J. y Zarzalejos Nieto, J. (2018). Aspectos fundamentales de derecho procesal penal. 4ª ed. Madrid: Wolkers Kluwer.

Gimeno Sendra, V. y Díaz Martínez, M. (2018). Manual de derecho procesal penal.2ª ed. Madrid: Ediciones Jurídicas Castillo de Luna.

González-Cuéllar Serrano, N. Y Gimeno Sendra, V. (1990). Proporcionalidad y derechos fundamentales en el proceso penal. Madrid: Ed. Colex.

Marchena Gómez, M., González-Cuéllar Serrano, N. (2015). La reforma de la Ley de enjuiciamiento criminal en 2015. Madrid: Ediciones Jurídicas Castillo de Luna.

Zaragoza Tejada, J y Bermúdez González, J. (2017). Investigación tecnológica y derechos fundamentales. Cizur Menor (Navarra): Aranzadi-Thomson Reuters.

REVISTA ACADÉMICA

Sánchez Gómez, R. (2016). El agente encubierto informático. La Ley Penal, nº 118 Sección Estudios, Enero-Febrero 2016.

LEGISLACIÓN

España. Constitución Española. (BOE 29 de diciembre de 1978)

España. Real Decreto de 14 de Septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (BOE 17 de septiembre de 1882)

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

España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (BOE 23 de noviembre de 1995)

Unión Europea. Declaración de aplicación provisional del Convenio de asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, hecho en Bruselas el 29 de mayo de 2000. (BOE 15 de octubre de 2003)

JURISPRUDENCIA

Sentencia de la Sala de lo Penal de la Audiencia Nacional 1519/2018 26 de abril.

Sentencia de la Sala de lo Penal de la Audiencia Nacional 3462/2018 del 25 de septiembre.

Sentencia del Tribunal Constitucional 173/2011 de 7 de noviembre.

Sentencia del Tribunal Constitucional 207/1996, de 16 de diciembre.

Sentencia del Tribunal Supremo. Sala Segunda 1140/2010 del 29 de diciembre.

Sentencia del Tribunal Supremo. Sala Segunda 767/2007 del 3 de octubre.

Sentencia del Tribunal Supremo. Sala Segunda 1166/2009 de 19 noviembre

Sentencia del Tribunal Supremo. Sala Segunda 690/2010, del 1 de julio.

Sentencia del Tribunal Supremo. Sala Segunda 360/2016, del 10 de febrero.

Sentencia del Tribunal Supremo. Sala Segunda 571/2008, del 25 de septiembre.

Sentencia del Tribunal Supremo. Sala Segunda 848/2003 del 13 de junio.

Sentencia del Tribunal Supremo. Sala Segunda 1992/1993 del 15 de septiembre.

Sentencia del Tribunal Supremo. Sala Segunda 342/2013, del 17 de abril.

Sentencia del Tribunal Supremo. Sala Segunda 655/2007 del 25 de junio.

RECURSOS ELECTRÓNICOS

Conde- Pumpido, P. (2015) "Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos" Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Comunicaci%C3%B3n%20Conde-Pumpido%20Garc%C3%ADa,%20Paloma.pdf?idFile=b243d8eb-4156-4d93-82b0-ccffc6992aa4 [Consulta 03 Nov. 2018].

Garberí, A. (2016). Comentarios sobre el Delito provocado - Doctrina Tribunal Supremo. [en línea] Garberí Penal. Disponible en: http://www.garberipenal.com/delito-provocado-practica-agente-encubierto/ [Consulta 26 Nov. 2018].

Gudín Rodríguez-Magariños, F. (2018). [en línea] Web.icam.es. Disponible en: http://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf [Consulta 03 Nov. 2018].

Jurado Fortes, M. (2018). Agente Encubierto Informático. [en línea] López de Lemus Abogados. Disponible en: https://lopezdelemus.com/agente-encubierto-informatico/ [Consulta 07 Nov. 2018].

Jurídicas, N. (2018). Contenido y novedades de la reforma de la LECrim por la Ley Orgánica 13/2015 y por la Ley 41/2015 · Noticias Jurídicas. [en línea] Noticias Jurídicas. Disponible en: http://noticias.juridicas.com/actualidad/noticias/10551-contenido-y-novedades-de-la-reforma-de-la-LECrimim-por-la-ley-organica-13-2015-y-por-la-ley-41-2015/ [Consulta 06 Nov. 2018].

MARTÍN-CARO SÁNCHEZ, J. (2015). Modificación de la Ley de Enjuiciamiento Criminal: sí, pero no. [en línea] Elnotario.es.Disponible en: http://www.elnotario.es/index.php/hemeroteca/revista-59/3976-modificacion-de-la-ley-de-enjuiciamiento-criminal-si-pero-no [Consulta 26 Nov. 2018].

Perals Calleja, J. (2010). El agente encubierto. la figura del arrepentido. protección de testigos. entrada y registro. apertura de correspondencia. [en línea] Fiscal.es. 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 [Consulta 01 Nov. 2018].

Valverde Megías, R. (2018). Cuestiones procesales relativas a la investigación de los delitos en red. [online] Fiscal.es. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Sr.%20VALVERDE.pdf?idFile=98ee6878-f370-403a-911b-7d71200a932a [Consulta 15 Nov. 2018].