Universitat Autònoma de Barcelona

Agente Encubierto Online

Autor: Àlex Cànovas Rodríguez

Grupo 51

4º curso

Director: Pedro Ruiz Soto

Fecha de entrega: 08/5/2017

Resumen

La reforma de la Ley de enjuiciamiento criminal llevada a cabo en 2015 introdujo una serie de nuevos apartados dirigidos a dar cabida al avance de las nuevas tecnologías en nuestro Ordenamiento jurídico. Veremos en este trabajo una de esas medidas: el agente encubierto informático, así como las dos medidas de investigación que he considerado más ligadas a ella: el rastreo de la IP y el registro remoto sobre equipos informáticos. Analizaremos pues, cuáles son sus características, sus requisitos y sus peculiaridades intentando arrojar luz sobre esta figura tan novedosa en nuestro ordenamiento jurídico. Indagaremos también en las diferentes opiniones de los profesionales de la materia y, si la encontramos, utilizaremos la jurisprudencia para acompañar todas las afirmaciones que vayamos aportando. Haremos especial mención a las peculiaridades de las pruebas informáticas que pueda recopilar el agente y el tratamiento que estas deben recibir para que sean válidas posteriormente en un proceso judicial penal. Por último haremos un cierre del trabajo ofreciendo unas conclusiones y una pequeña visión crítica personal sobre todo lo que hayamos visto durante todo el trabajo.

The Law reform on criminal prosecution carried out in 2015 introduced a series of new sections aimed at accommodating the advance of new technologies in our legal system. We will see in this work one of these measures: the undercover computer agent, as well as the two research measures that I have considered most related to it: IP tracking and remote registration on computer equipment. We will see, what are their characteristics, their requirements and their peculiarities trying to shed light on this recent figure in our legal system. We will also inquire into the different opinions of the subject professionals and, if we find it, we will use the jurisprudence to accompany all the affirmations that we are contributing. We will make special mention of computer evidences peculiarities that the agent can collect and the treatment that they must receive in order to be valid afterwards in a criminal judicial process. Finally we will do a closing of the work offering conclusions and a small personal critical vision on everything that we have seen during all the work.

Índice Agente Encubierto Online

Abreviaturas

- Art. Artículo
- IP Internal Protocol
- Lecrim Ley de Enjuiciamiento Criminal
- OJ Ordenamiento Jurídico
- SAN Sentencia Audiencia Nacional
- STS Sentencia del Tribunal Supremo

Agente encubierto online

1. Presentación

En el presente trabajo estudiaremos los perfiles de una técnica de investigación a la que ha dado carta de naturaleza la última reforma de la LECRIM: el agente encubierto informático. Como apasionado de la informática y las nuevas tecnologías, esta reforma es un soplo de aire para las técnicas de investigación que llevan a cabo los cuerpos policiales de nuestro país.

Las formas de delincuencia han avanzado mucho junto con la tecnología y estos nuevos delitos informáticos han obligado a nuestro sistema a buscar nuevas formas de prevención de los mismos. Es innegable que la evolución informática está creciendo de manera exponencial y que cada vez encontramos nuevas maneras de superarla. Las posibilidades que nos ofrece hoy en día la red son casi ilimitadas y la característica más singular que tiene la red es el anonimato. Por desgracia muchas veces este anonimato o la sensación del mismo nos lleva a situaciones realmente difíciles para perseguir a las personas que no hacen un buen uso de internet.

El número de páginas web que podemos encontrar es casi infinita y es imposible mantener un control efectivo sobre todas ellas. El desconocimiento sobre el vasto dominio virtual nos demuestran que internet sigue siendo un misterio para la gente de a pie aunque lo utilicen diariamente. Hay miles de formas de esconderse que permiten eludir los controles policiales, resultando mucho más sencillo saltarse la ley. Por este motivo hemos tenido que dar un salto importante en nuestra legislación y crear nuevas formas de control adaptadas al crecimiento informático. El agente encubierto online junto con otras dos diligencias de investigación (registro remoto sobre equipos informáticos y rastreo de la dirección IP) que veremos y trataremos en el trabajo son verdaderas actualizaciones, en el sentido más informático de la palabra, de otras diligencias que ya existían para poder compatibilizar la investigación con el vasto mundo virtual.

Aunque parezca una reforma que intenta introducir la tecnología en nuestro ordenamiento jurídico y en la actividad de investigación, lo cierto es que la convivencia entre tecnología e investigación siempre ha existido.

Técnicas como la intervención de llamadas telefónicas, balizas de seguimiento o utilización de todo tipo de aparatos tecnológicos avanzados son ya antiguas en nuestra regulación, por lo que podríamos desmentir la idea general de que nuestro ordenamiento jurídico no atiende a los recientes avances tecnológicos. De todos los nuevos métodos introducidos en la reforma nos centraremos en la figura del agente encubierto online la cual está orientada a descubrir actividades criminales que repugnan a la mayoría de la sociedad y lesionan muy gravemente los bienes jurídicos protegidos por el derecho penal como la persecución de la pornografía infantil o hasta incluso la captación de miembros en bandas terroristas.

Haremos un pequeño repaso histórico de la figura del agente encubierto físico para ver cómo ha evolucionado esta técnica y que tan buenos resultados ha obtenido. Veremos cuáles son sus cualidades y sus defectos, así como su regulación tan novedosa la cual parece que ha generado múltiples debates en la doctrina por ser poco precisa o incompleta.

Veremos también dos diligencias de investigación que a mi parecer están totalmente ligadas a la figura principal del agente encubierto virtual, a saber la innovadora medida conocida como registro remoto sobre equipos informáticos, la cual genera muchísimas preguntas y la no tan novedosa medida de rastreo de la dirección IP, con un debate, en mi opinión, muy interesante.

Por último también daremos una visión específica de la cadena de custodia en relación a las pruebas informáticas. Veremos que no podemos tratar de la misma forma una prueba informática que a una prueba física y que necesitaremos seguir un proceso más acorde con sus características.

2. Antecedentes: el agente encubierto en el mundo físico y límites de su actuación

Como ya sabemos, durante toda la historia de la humanidad, la información ha significado poder. Muchos de los avances más grandes en nuestra sociedad han estado ligados por tener información a nuestra disposición. El agente encubierto nace de esta necesidad de encontrar información en un ámbito donde el poder del Estado o de las fuerzas de seguridad se ve sobrepasado: las organizaciones criminales. Con la misma intención podemos buscar una figura parecida en los más importantes estadios de la humanidad. Los espías eran una parte esencial de las tácticas bélicas tanto en Grecia, Roma, la Europa Feudal como en otros territorios más alejados de nuestra cultura como Asia[1]. Buscar información sobre pueblos rivales a los que se quería conquistar formaba parte de una táctica militar muy extendida en estos periodos. Pero estas figuras, aunque son un ejemplo de la idea básica que busca el agente encubierto (buscar información para identificar al enemigo), distan demasiado de la figura que conocemos actualmente.

Se podría decir que el primer antecedente claro lo encontramos en el régimen totalitario de Luís XIV en Francia. En este periodo no se distingue como se hace hoy en día entre el agente provocador y el agente infiltrado, a los que recurriremos más adelante, pero vemos una figura encargada de dar información de las actividades ilegales al poder estatal. Los denominados *"mouches"*[2] daban información a los cuerpos policiales franceses del siglo XVIII sobre las actividades ilegales, tales como timbas, prensa ilícita o actos contra el poder entre otros, que tenían lugar en las zonas poco controladas por la policía. Estos sujetos no eran agentes policiales, sino personas que solían frecuentar estos lugares. No tenían consideración de agente público pero si estaban bajo el control de estos (generalmente se negociaba con los delincuentes este tipo de cooperación para retirar su condena o al menos rebajarla).

[1] Ya se hace referencia a la figura del espía en el escrito: "*El arte de la Guerra*" de Sun Tzu, ubicado en el siglo IV a.C.

[2] "moscas" en español. Con esto podemos ver la consideración callejera y suburbana que tenían estos sujetos.

Esta actividad se fue acrecentando de manera que aparecieron los llamados "delatores", los cuales se dedicaban especialmente a informar al príncipe sobre tales actividades a cambio de favores, huyendo así de los sujetos más problemáticos y de la provocación para cometer delito y empezando a vislumbrar una institucionalización de la técnica.

También hay constancia de otras prácticas similares en otros lugares del mundo como por ejemplo Estados Unidos con el llamado *"Italian Squad"*, un comando creado en 1906 para detener a la Camorra italiana en Estados Unidos y dirigidos por el agente Giuseppe "Joe" Petrosino. Este agente infiltrado descubrió más de 75 personas que fueron arrestadas por el cuerpo policial. Lamentablemente su identidad salió a la luz a través de un diario y fue asesinado en 1909 en Sicilia durante una investigación. Aun así su unidad siguió operando y luchando contra el crimen organizado hasta 1922, año en el que *Italian Squad* fue desmantelado. [3]

Queda claro pues, que esta figura del agente encubierto se utiliza para enfrentarse a amenazas de las que el Estado no puede actuar con comodidad porque carece de información sobre el funcionamiento y operativa interna de las organizaciones criminales. Uno de los puntos donde más ha sufrido esta desigualdad, no solo en nuestro Estado, sino en muchas potencias mundiales, es el tráfico de estupefacientes. Aquí es donde la figura del agente encubierto empieza a verse como indispensable a nivel procesal. Aun así, es cierto que esta medida restringe fuertemente los derechos fundamentales de las personas y por ello necesita una fuerte regulación con unos límites estrictos. El agente encubierto no aparece en nuestra Ley de Enjuiciamiento criminal hasta la reforma por la Ley Orgánica 5/1999, de 13 de enero, en la que se incluirá el art. 282 bis y con él la figura del agente encubierto. Una vez incluido en nuestro OJ, el art. 282 bis impone unos requisitos y límites a la actuación policial.

En primer lugar la ley fija un requisito esencial para poder acudir a esta técnica: la autorización judicial. Solo el juez de instrucción o el Ministerio Fiscal dando cuenta inmediata al juez tiene la potestad para aplicar esta medida, con lo cual retiramos la libre actuación de los cuerpos policiales para procurar una mejor protección de los derechos fundamentales.

[3] "The Italian Squad, NYPD" Chronicling America: American Historic Newspapers digital collection https://www.loc.gov/rr/news/topics/italian.html

Con esta autorización también otorgan al agente en cuestión la protección legal - impunidad - en relación a los posibles delitos en los que pueda concurrir durante su actuación, permitiendo así *" a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos"*. También a su vez se le creará una identidad supuesta (identificación falsa) que le acompañará durante toda la investigación y que podrá mantener incluso durante todo el proceso judicial para mantener su seguridad personal. A esto se debe añadir, que la medida tendrá un tiempo límite de 6 meses, aunque se podrá prorrogar por la misma cantidad de tiempo de forma indefinida (siempre manteniendo los principios de proporcionalidad y de mínima intervención).

El otro gran límite a la actuación es el requisito por el que solo se permite la actuación del agente encubierto en casos de delincuencia organizada, a saber: *"la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes"* Estos delitos de los que nos habla la ley serían 11 originalmente y con las reformas de 2003 y 2010 se añadirían 4 grupos de delitos más (1 y 3 en cada reforma respectivamente). Por lo tanto esto significa que los delitos están expuestos en una lista cerrada de modo que no podemos perseguir cualquier tipo de delito. Aun así los delitos incluidos en la lista son los más representativos de las organizaciones criminales y podemos encontrar entre ellos el secuestro de seres humanos, la trata de seres humanos, prostitución, tráfico de armas o delitos contra la salud pública entre otros.

Generalmente los delitos en los que más frecuentemente ha intervenido el agente encubierto siempre han sido la persecución de narcotraficantes (los cuales no solo cometen delitos de tráfico de estupefacientes), debido a la gran cantidad de recursos que estos tienen y a la dificultad para obtener pruebas o evidencias.

Además estos criminales suelen actuar en distintos territorios, lo que todavía dificulta más esta la investigación. Resulta claro que la figura del agente encubierto es clave para destapar estas actividades y conseguir pruebas suficientes para encausar al supuesto criminal, además, los narcotraficantes importantes no suelen trabajar solos por lo que no encontramos grandes problemas para determinar la actividad organizada en estos casos.

Por último un límite muy interesante y problemático se debe al apartado nº 5 del propio artículo 282 bis: se le prohíbe al agente provocar el delito. Explicaremos ampliamente este apartado más adelante en el trabajo, dedicándole un apartado exclusivo. Para explicar este apartado será necesario atender a la diferencia entre el agente provocador y el agente infiltrado mencionada al inicio del estudio histórico del trabajo.

Todo ello configura la historia y los límites del agente encubierto, pero como bien adelantábamos, en 2015 tenemos una nueva reforma para dar cabida a un nuevo paso en la evolución de esta figura. La Ley Orgánica 13/2015, de 5 de octubre, introduce en nuestra Lecrim las previsiones necesarias para integrar las nuevas técnicas y formas de infiltración en nuestro ordenamiento. Se crea de este modo una nueva modalidad conocida como el agente encubierto informático.

3. El agente encubierto virtual: art. 282 bis

El siguiente paso en la historia del agente encubierto es, como ya he dicho, muy reciente. Una de las nuevas técnicas de investigación más útiles y a la vez controvertida de la reforma de la Lecrim es el agente encubierto informático[4]. Como su nombre indica se trata de un agente policial encargado de investigar y descubrir posibles delitos que se cometen en la red y especialmente ha tenido un amplio éxito en la investigación de delitos relacionados con la pornografía infantil y la lucha contra el terrorismo al poder detectar estos individuos en los principales canales de comunicación que utilizan. Como ya hemos visto, la figura del agente encubierto entró en el OJ español con la reforma introducida por la Ley Orgánica 5/1999, de 13 de enero.

Con el paso de los años, las nuevas tecnologías entraron en nuestras vidas y con ellas una nueva forma de cometer delitos con una dificultad añadida la cual generaba una frecuente impunidad. La utilización del agente encubierto quedaba muy anticuada para perseguir ciertos delitos cometidos a través de la red, en su mayor parte delitos de pornografía infantil o relacionados con la pederastia y muchas actuaciones de grupos terroristas, captando a jóvenes y creando así nuevos seguidores sin necesidad de estar físicamente presente. Surge así la necesidad de regular una nueva función para este agente y así actualizarlo (en el sentido literal) para poder cubrir un terreno difícil de controlar, facilitando a su vez el control sobre delitos de estafas cometidas a través de internet o de daños a equipos informáticos. Se crea así la figura del agente encubierto informático, introducido en nuestro ordenamiento jurídico con la reforma de la Ley Orgánica 13/2015, de 5 de octubre. Es importante destacar también, que el Tribunal Supremo ya había reconocido anteriormente la existencia de esta práctica policial (STS 767/2007 de 3 octubre), aunque no la trataba como una diligencia excepcional o individual sino como una práctica propia de los agentes policiales para hacer su labor de investigación o como una práctica ordinaria del agente encubierto originariamente previsto.

[4] El cual podemos encontrar también como agente encubierto on line, virtual o hasta incluso agente encubierto 2.0.

4. Problemática en la aplicación del agente encubierto informático

1. El requisito de la organización criminal

La Lecrim, en su artículo 282 bis, como ya hemos visto, establece unos requisitos muy estrictos para poder usar la figura del agente encubierto en una investigación; recordemos la necesidad de la autorización judicial y además una actividad de información por parte del agente (siempre que sea posible) constante, dando cuenta al juez de instrucción de todas las investigaciones o descubrimientos que se hayan efectuado. Todos estos requisitos se deben mantener para efectuar una investigación a través del agente encubierto informático.

El primer problema importante lo encontramos ante el requisito referido a la actividad criminal organizada. La ley deja claro desde el primer momento que solo se podrá actuar *"cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada"*. Como ya sabemos este requisito encajaba muy bien en las funciones del agente encubierto original, puesto que era difícil encontrar un supuesto de la lista proporcionada por la ley (apartado 4 del art. 282 bis) que fuera lo suficientemente grave y que no estuviera relacionado con alguna organización criminal.

Pero con el avance del tiempo la investigación de los delitos obtuvo un nuevo enfoque con la aparición de las nuevas tecnologías y de sus amplias posibilidades. Parecería razonable pensar que la actuación virtual de un agente encubierto funciona del mismo modo que el agente encubierto corriente, pero es cierto que muchos de estos delitos que se cometen aprovechando las posibilidades que ofrece la informática no responden a la condición requerida por la ley: que sean delitos cometidos en el seno de una organización criminal.

En general estas actividades ilícitas cometidas a través de la red, no tienen un encaje en el concepto de delincuencia organizada o delitos cometidos por una organización criminal. Los delitos relativos a la pornografía infantil por ejemplo, se suelen producir en distintas redes sociales o chats privados en los que no existe una organización ni un reparto de tareas distinguido.

Simplemente se produce una comunicación con otros internautas que llegaban a contactar con ese individuo de modo fortuito o por la simple comunicación que les permite la web, pero en muy pocos casos se podría contemplar un concierto previo ni una organización. Lo mismo ocurrirá cuando en los delitos de captación en los grupos terroristas cuando la persona que capta nuevos miembros lo hace de manera individual y personal. De hecho es bastante frecuente que muchos integrantes de la yihad busquen a otros miembros sin necesidad de recibir órdenes o instrucciones. Cabe mencionar también el delito del hacking, el cual no veremos durante el trabajo, pero también tiene como característica la actuación individual (aunque a veces sí se dan casos de grupos organizados) y sigue siendo un delito grave, por su frecuencia y sus efectos, cometido a través de la red.

Esta situación podría llegar a excluir estos delitos de la investigación por parte de un agente encubierto informático, pero si analizamos alguna jurisprudencia del Tribunal Supremo, veremos que esto ya ha planteado dudas y se ha resuelto con un argumento muy sólido.

Anteriormente el Tribunal Supremo se ha pronunciado en algunas ocasiones sobre la concepción de este tipo de redes; una de las resoluciones más importantes que podríamos encontrar, sería la STS 1444/04, de 10 de diciembre[5] en la cual se aplica una agravante por delincuencia organizada para un caso similar al que estamos trabajando. Para ello el Tribunal expone: *"Lo esencial en estos nuevos fenómenos delictivos está, precisamente, en que la simple utilización de la red de comunicaciones informáticas supone ya el aporte del elemento de coordinación y el empleo de medio excepcional que se proyecta hacia una mayor lesividad, imprescindibles, aunque no del todo suficientes, para la consideración de la existencia de una organización criminal."* Como vemos el tribunal no lo determina como un elemento decisivo pero si muy importante para considerar estas actividades como delincuencia organizada.

Con este razonamiento podemos afirmar que si es una actividad subsumible en el art. 189.2 apartado f del Código Penal, es decir, un agravante por pertenecer a una organización o asociación delictiva, podría ser considerada con el mismo argumento para cumplir el requisito del art. 282 bis Lecrim.

[5] Ratificada por otras sentencias un poco más actuales como la STS 739/2008 de 12 noviembre.

Aún así no creo que se pueda asegurar totalmente esta relación puesto que en la misma sentencia ya nos advierte de lo siguiente: *"No es lo mismo, por tanto, ni merece igual consideración punitiva, la conducta del infractor aislado que capta, elabora y distribuye por sí solo material pornográfico, incluso mediante INTERNET, que el supuesto de hallarnos ante una pluralidad de usuarios que, coincidentes en ese «lugar de encuentro» virtual, coordinan sus acciones para potenciar las posibilidades de consumo de las imágenes dañinas para los derechos de los menores, permitiendo, además, su difusión incluso a otras personas ajenas al grupo organizado."*

Entiendo por tanto, que esta actividad debe ser conjunta, con intervención coordinada de varios sujetos, aunque no haya una organización clara o no intuyamos una colaboración activa. Ciertamente pienso que es un argumento un tanto forzado, es decir, me cuesta creer que nuestro Código Penal tuviera en mente este tipo de organización. Generalmente para considerar como grupo criminal a una pluralidad de personas, se requiere organización, distribución de funciones o algún tipo de cadena de mando. En los delitos de terrorismo no se presentaba este problema, pero en los delitos de pornografía infantil es inusual ver estos rasgos. El compartir archivos entre un número elevado de personas no requiere ningún tipo de organización ni reparto de tareas, no veo en estos casos, argumentos suficientes para determinar la organización del grupo. Si bien es cierto que en la sentencia que acabamos de comentar matiza este concepto y deja claro que necesitaremos una coordinación de funciones, no creo que esta coordinación se dé simplemente por la comunicación vía internet como dice la sentencia.

Cabría pensar a partir de este texto que la actividad individual de un sujeto que hace personalmente todas las funciones necesarias para cometer el delito no revestirá de la consideración de organización criminal, aunque luego distribuya este material a otros sujetos desconocidos.

De todos modos otra posible solución a este problema es que deberíamos plantearnos si es verdaderamente necesario este requisito de crimen organizado. La comentada reforma introducida por la Ley Orgánica 13/2015, de 5 de octubre que introducía los apartados 6 y 7 del actual art. 282 bis Lecrim, en la cual se introduce la figura que estamos estudiando, parecía ir dirigida (entre otros objetivos) a facilitar la investigación y frenar así los delitos cometidos a través de las redes.

En su exposición de motivos, considerando IV, se vislumbra una pequeña referencia a la persecución especialmente destinada a la pederastia o pornografía infantil[6]. Según su propia exposición de motivos, esta reforma nos servirá para introducir la figura del agente encubierto informático en nuestro cuerpo legal y así tener más herramientas para frenar dichas actividades o al menos localizarlas con más facilidad, lo que no deja del todo claro es si seguirá aplicándose el controvertido requisito del crimen organizado.

No tenemos a día de hoy ninguna sentencia que arroje luz sobre esta duda pero sin embargo, según el estudio de Javier Ignacio Zaragoza Tejada[7], el apartado nº 6 del art. 282 bis permitiría al juez de instrucción acordar la medida del agente encubierto fuera de los casos de las organizaciones criminales y usarlo para canales cerrados de comunicación (chats virtuales por ejemplo) sin que exista por tanto esa nota de cooperación u organización, atendiendo como es lógico, a los criterios como la proporcionalidad y la idoneidad para no caer en la dinámica de perseguir delitos poco relevantes o poco lesivos socialmente.

Para el resto de criterios requeridos por la ley para el uso de esta figura parece que no habría distinción con los del agente encubierto ordinario.

2. Distinción de la función de cibervigilancia

Sin embargo, la técnica del agente encubierto online plantea otros problemas que podrían afectar a su validez. Entre las funciones policiales siempre hemos encontrado la de ejercer un control ciudadano en todos los ámbitos posibles, ya sea a pie de calle, en grandes eventos, controles de tráfico, y un largo etcétera. Esta vigilancia o control también se efectúa en las redes, sin necesidad de ningún tipo de resolución judicial que lo permita.

La presente situación desarrolla una problemática importante al establecer la frontera entre esta función de control propia de los cuerpos de seguridad, establecida en el artículo 11 de la Ley de Fuerzas y Cuerpos de Seguridad, y la actividad que ejerce un agente encubierto online cumpliendo con la orden dictada por el juez de instrucción.

[6] En ningún caso habla de estos delitos de forma específica pero si hace alusión a prácticas frecuentes en estos delitos como intercambiar imágenes o archivos

[7] ZARAGOZA TEJADA, Javier Ignacio, El agente encubierto online: la última frontera de la investigación penal. Revista Aranzadi Doctrinal num.1/2017 parte Tribuna. Editorial Aranzadi, S.A.U., Cizur Menor. 2017.

Incluso podríamos forzar más el límite si vemos específicamente las actividades de la policía judicial establecidas en el art. 282. La posición de la frontera entre estas dos actividades será extremadamente importante para la validez de la investigación puesto que para el "*ciberpatrullaje*[8]*"* no se requiere autorización judicial, pero sin embargo sí se requiere para la actuación del agente encubierto online.

La problemática se da porque estos canales de comunicación son en su mayoría accesibles para todo el mundo, es decir, cualquier persona puede acceder a ellos de manera anónima[9], aunque generalmente será necesario un registro. Podríamos pensar que este registro lo convierte en un chat íntimo o privado pero no parece un argumento muy convincente, ya que otras redes ampliamente controladas por los cuerpos de seguridad (como Facebook por ejemplo) también requieren un registro previo. Hemos de entender que el registro es un mero trámite con el que no se te obliga a dar una identificación fehaciente ni unos datos reales, por lo que podríamos entender que las funciones de control parecen ser mínimas o directamente inexistentes.

La controversia se acrecentaría para determinar si las funciones de control tienen el límite en:

1. El simple acceso a estos chats, creando una cuenta en ellos para poder ver conversaciones sin participar;
2. llegar a entablar una conversación con un supuesto delincuente sin indicios claros de su actividad ilícita;
3. establecer una comunicación estable durante un periodo amplio para investigar al sujeto teniendo sospechas muy fundadas de su supuesta actividad ilegal;
4. Recibir archivos ilícitos de este sujeto investigado o
5. Intercambiar o subir archivos ilícitos en la red.

Podemos descartar con seguridad el último punto. Subir o intercambiar archivos ilícitos quedaría totalmente fuera de la legalidad para la modalidad del ciberpatrullaje puesto que se trata de una actividad ilícita, que podría generar responsabilidad penal.

[8] Término utilizado por el propio Javier Ignacio Zaragoza.

[9] hay que matizar que este tipo de chats suelen estar ubicados en la deepweb lo cual dificulta mucho su búsqueda. La deepweb son todas aquellas páginas web que no están indexadas por un buscador como Google o Bing y que por lo tanto sólo se puede acceder a ellas mediante la dirección o url. Dentro de la deepweb encontramos a su vez la darkweb a la cual sólo se podrá acceder mediante la dirección y el permiso del autor de la misma.

Sin una autorización judicial expresa parece imposible que nuestro ordenamiento jurídico permita actividades ilícitas por parte de los cuerpos de seguridad. Necesitaremos un control judicial para ello, control que no tiene el ciberpatrullaje. En este caso tenemos una sentencia del Tribunal Supremo[10], que aunque sea anterior a la reforma de la Lecrim y no distinga esta figura de la del agente encubierto ordinario, expone muy bien la situación del límite de actuación del ciberpatrullaje. Parece ser que el límite lo estableceríamos entre el segundo y tercer punto, es decir, cuando el agente (sin ser aún encubierto) descubre comportamientos sospechosos que le hacen pensar racionalmente que el investigado podría estar cometiendo actividades ilícitas. Es posible que llegue a recibir archivos de la persona investigada, pero entiendo que no debería ser la norma general. Aun así, si llegara a ocurrir que el investigado compartiera un archivo ilícito sin que el agente lo requiriera, la correcta actuación sería poner el caso en manos de un juez de instrucción para que este autorice al agente a mantener la conversación con el investigado y a su vez permita al agente ahora sí recibir e intercambiar archivos para ganarse la confianza del sujeto en cuestión.

Así lo expone el TS cuando dice: *"Efectivamente, lo cierto es que los agentes de la autoridad, cuando realizan las labores habituales de vigilancia para prevenir la delincuencia informática tuvieron noticia casual de la existencia de un posible delito de difusión de pornografía infantil. 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 donde se instruyeron las pertinentes diligencias informativas y, acto seguido, tras la denuncia en el Juzgado de Instrucción, las Diligencias Previas."*

Verdaderamente debemos admitir que a priori parece extraño (aun más cuando no teníamos la reforma de la Lecrim) pensar que un agente, sin autorización judicial pueda introducirse en un canal de comunicación virtual, utilizando un nombre falso y entablando conversación con desconocidos para investigar supuestos delitos.

Es interesante para resolver esta cuestión la falta de identificación tan característica en el mundo virtual en el cual se mueve el agente.

[10] STS num. 767/2007 de 3 octubre de 2007

Esto permite al agente crear una cuenta, con un nombre manifiestamente falso sin ningún tipo de problema, ya que el otro interlocutor sabe sin lugar a dudas que ese no es su nombre real y por supuesto él tampoco dará su nombre real. Es la norma general en la red y a la vez es uno de los motivos por los que no es necesaria la autorización del juez de instrucción, porque en realidad no tenemos una identificación falsa sino un "*nick*" o un apodo propio de los chats virtuales.

Con este razonamiento podemos entender por qué no es necesaria la autorización de un juez para entrar en dichos chats, porque efectivamente, aunque se cree una identidad "falsa" o "supuesta", entra dentro de la cotidianidad dentro de la red.

3. Delito provocado y delito comprobado

Retomamos esta problemática que tanto ha afectado a las distintas actuaciones del agente encubierto físico y que probablemente también afecte notablemente a la actuación del agente encubierto online. El agente provocador crea un dolo en la persona que se está investigando para así someterlo a la acción de la justicia. Inicialmente, en la concepción francesa de "*mouches*" que hemos visto anteriormente, esta práctica era aceptada y no presentaba problemas; hoy en día no se puede aceptar como prueba algo que se ha inducido a hacer. El agente infiltrado por otro lado no provoca ningún tipo de dolo, simplemente se limita a informar de las actividades ilícitas que se desarrollan, pudiendo participar en ellas pero nunca llegar a provocarlas.

Esta diferenciación es extremadamente importante puesto que la inducción del agente a cometer el delito significará la absolución del mismo. Hay muchísima jurisprudencia sobre este asunto y por lo tanto es un concepto bastante cerrado, con grandes aportaciones del Tribunal Supremo. Veremos diversos ejemplos distribuidos en un amplio abanico de tiempo acudiendo a la jurisprudencia del Tribunal Supremo.

Encontramos una buena explicación de este "delito provocado" en la STS 1110/2004 de 5 octubre (RJ 2004\6548)[11]: *"El delito provocado, que conlleva la impunidad de la acción típica, es aquél que sólo llega a realizarse en virtud de la inducción eficaz de un agente (el agente provocador) que, ha generado con su actuación engañosa la idea delictiva del autor, anteriormente inexistente, y la ejecución de la conducta ilícita, considerándose que en estos casos la infracción es impune porque carece de realidad, es pura ficción, ya que es el representante de la Autoridad el que quiso que la norma penal fuera conculcada y su actuación fue esencial, determinante y decisiva para ello [...]"* . Como podemos ver, la visión del tribunal intenta ser favorable a la actuación del agente, dejando amplios márgenes para su actuación.

Incluso en esta misma sentencia, el Tribunal Supremo nos habla de los "delitos comprobados", ya reconocido en una amplia jurisprudencia. Con este término, el tribunal explica que es distinta la provocación para delinquir instando al investigado a cometer una conducta ilícita, de aquella conducta llevada a cabo por el agente infiltrado para descubrir delitos de trato sucesivo y que por lo tanto se cometen al margen de su voluntad. Volveremos a esta distinción más adelante.

Concretamente el Tribunal lo describe de la siguiente forma: *"tiene lugar cuando la actividad policial, sin quebrar legalidad alguna, pretende descubrir delitos ya cometidos, generalmente de tracto sucesivo, como suelen ser los de tráfico de drogas, toda vez que en estos supuestos el agente infiltrado no busca ni genera la comisión del delito, sino allegar las pruebas de una ilícita actividad ya cometida o que se está produciendo, pero de la que únicamente se abrigan sospechas."*

Como podemos ver, es muy importante que la actuación del agente sea correcta y que se aleje de la figura del agente provocador. Por ejemplo en la SAN núm. 53/2010 de 5 julio. ARP 2010\845 se considera delito provocado y como consecuencia se produce la absolución del investigado por tráfico de estupefacientes, a causa de la atipicidad de su conducta, fruto de una mala actuación policial. Las pruebas que hayan sido recabadas usando un agente que haya provocado el delito no podrán ser consideradas como válidas y es muy posible que destruya toda una investigación posterior.

[11] Entre muchas otras más sentencias como por ejemplo SSTS de 19 de noviembre de 2009 o de 22 de junio de 1994

Será necesario por tanto, distinguir entre la acción que provoca el delito y la acción que, una vez demostrado el delito, solo prueba la existencia del mismo. Ciertamente el agente encubierto informático es demasiado reciente para que tengamos jurisprudencia que nos explique los límites de su actuación de suerte que intentaremos extraer las bases del delito provocado y extrapolarlas hacia el mundo virtual y la acción del agente informático.

Acudiremos ahora a una sentencia más antigua, en la que ya se mencionan las directrices para poder entender la distinción entre delito provocado y delito comprobado. La sentencia en cuestión es de 1992[12] en la que ya se reconoce esta discusión doctrinal, luego el debate ya estaba abierto.

En dicha sentencia ya nos habla de la figura del delito comprobado aunque muy someramente y no lo llama por ningún nombre, simplemente lo describe: *"su conducta reconocía una influencia y un interés desvinculados de la actuación del agente provocador [...]"*

Damos un salto en el tiempo y acudimos a una sentencia más actual, concretamente la Sentencia núm. 253/2015 de 24 abril[13], en la que nos define mejor como distinguir entre el delito comprobado y el delito provocado.

Para el Tribunal el delito provocado consta de tres características:

"El delito provocado se integra por tres elementos:

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

[12] STS núm. 1672/1992 de 10 julio. RJ 1992\6665

[13] STS núm. 253/2015 de 24 abril RJ\2015\1866

Con este esquema, dirigido a delimitar el delito provocado en acciones relativas al tráfico de droga, podemos extraer la esencia y aplicarla a los delitos más frecuentes con los que se topa el agente encubierto informático: los delitos de pornografía infantil y los relativos al terrorismo.

Como ya sabemos, el agente encubierto virtual puede intercambiar ficheros con supuestos delincuentes para así ganarse su confianza y llegar a pedir que le "devuelva el favor" pidiendo a cambio más archivos que el investigado pueda poseer. Si el agente directamente pidiera estos archivos a una persona y esta los entregara podría generar dudas acerca de si ha existido una provocación para cometer el delito. Se cumplirían los tres requisitos vistos en la sentencia y en consecuencia, todas las pruebas derivadas de esa acción podrían resultar nulas.

Para la correcta utilización de dicha medida hará falta una seguridad sobre la conducta ilícita del investigado. En definitiva, siguiendo la lógica aplicada por el Tribunal Supremo[14], la distinción radicará principalmente en averiguar cuál era la actitud del investigado inicialmente, es decir, si efectivamente el agente ha creado un dolo antes inexistente o si por el contrario, el dolo ya existía anteriormente.

Para demostrar este dolo anterior serán necesarias pruebas suficientes para demostrar que el sujeto ya había llevado a cabo ese comportamiento en el pasado o incluso en el presente. El simple hecho de tener gran cantidad de imágenes almacenadas o la clasificación de éstas, de manera que permita una mayor rapidez en el momento de buscar un contenido concreto, e incluso rastrear la imagen para averiguar quién la ha descargado y desde donde, podrían ser clave para determinar las intenciones que tenía el investigado antes de la interacción con el agente.

Como ya digo, ningún Tribunal se ha manifestado todavía sobre este asunto específicamente pero creo que, en su momento, serán estos mismos criterios que habrán de emplearse para diferenciar, en el ámbito de las investigaciones tecnológicas, entre el agente encubierto y la provocación delictiva.

[14] STS núm. 253/2015 de 24 abril RJ\2015\1866

4. Archivos transferidos ¿controladamente?

Otro de los problemas que ha planteado esta medida es la posibilidad de transferir archivos ilícitos a los usuarios que están bajo investigación. A priori parece algo corriente en la actuación de un agente encubierto pero veremos a continuación que estos archivos ilícitos son más problemáticos. En un inicio el agente encubierto se ocupaba mayoritariamente de delitos contra la salud pública, es decir, tráfico de drogas. Para hacer mejor su función y evitar que fuera descubierto, se le permitía manejar paquetes de droga e incluso hacer envíos controlados. Esta práctica estaba admitida por la ley y la jurisprudencia porque no llegaba a lesionar ningún bien jurídico, de modo que la droga que se enviaba estaba totalmente controlada por la policía y no llegaba (o al menos esa era la intención) a manos del "consumidor". También hemos de tener en cuenta la exención de delito en ciertos comportamientos que son tomados como prueba para entrar en una banda, esto es, cuando en determinados grupos criminales (generalmente bandas callejeras) se le pide a los nuevos integrantes que realicen una prueba consistente en la comisión de un delito.

Todo ello será posible gracias al apartado 5º del propio artículo 282 bis de la Lecrim: *"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 la misma y no constituyan una provocación al delito."* Con este apartado, permitimos al agente encubierto tener más margen en caso de que deba cometer delitos y en definitiva se vuelve la característica más definidora que separa una actuación policial ordinaria (en la que puede haber ocultación) y una operación con agente encubierto.

Con la introducción del agente encubierto virtual se intenta asimilar estas dos exclusiones de la responsabilidad penal para permitir al agente intercambiar archivos con el investigado, de forma que se pueda ejercer un control sobre estos archivos y tampoco lleguen a lesionar ningún bien jurídico o sirvan para introducirse en un grupo que requiera aportaciones para entrar. Pero en la práctica esto no es tan fácil.

Como podemos ver en el art. 282 bis apartado 6º el juez de instrucción puede permitir al agente intercambiar archivos ilícitos y así analizar "los resultados de los algoritmos". Hasta aquí, la medida presenta diversos problemas.

El primero de ellos es que la ley en ningún momento da una definición por lo que entiende por algoritmos o nos explica en qué consiste el procedimiento. Si nos remitimos pues a una definición neutra (DRAE) nos encontramos con: "Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema". Creo que podemos determinar sin lugar a dudas esta definición no encaja muy bien con el precepto legal, luego tampoco nos servirá para interpretar lo que nos quiere decir el legislador. Por lo tanto, este procedimiento queda a merced de interpretación personal, creando inseguridad jurídica hasta que el Tribunal Supremo se pronuncie y fije una definición.

Por otro lado también hay distintas críticas acerca del posible almacenamiento de ese archivo. Imaginemos la situación en la que un ciudadano entra en el radar policial sin ser este un delincuente verdaderamente, y que por este motivo, se le manda un archivo ilícito por parte de la propia policía. Es una técnica prevista por la propia ley, por lo que si la policía tiene sospechas acerca de este individuo, actuará conforme a los límites que nos ofrece la Lecrim.

Si al final el investigado resulta culpable, esta actuación cobra un sentido, pero la policía, igual que todos, puede equivocarse y investigar a una persona que es inocente. Acto seguido, la policía sigue investigando y se le hace un registro domiciliario donde se encuentra el archivo que la propia policía le había enviado en su ordenador. Como bien indica *Javier Rubio Alamillo*[15] si no se tiene un buen control y un inventario sobre estos archivos puede desencadenar consecuencias muy graves para el investigado.

Aunque no considero este como uno de los problemas más graves, si me parece que la ley no dice nada acerca de esta situación y que la praxis ejecutada por la policía puede tener defectos; defectos que pueden condenar a una persona inocente o incluso puede poner en serios problemas al agente por estar induciendo al sujeto a delinquir considerando la acción como un delito provocado. También se me plantea el problema moral de escoger estas fotografías cuando hablamos de pornografía infantil. Desconozco el método que utilizarán para seleccionar las que son aptas para el envío en el curso de una investigación, pero como poco es alarmante que la policía pueda manejar fotografías infantiles pornográficas y que se puedan transferir posteriormente.

[15] RUBIO ALAMILLO, Javier, "La Informática en la reforma de la Ley de Enjuiciamiento Criminal" http://peritoinformaticocolegiado.es/la-informatica-en-la-reforma-de-la-ley-de-enjuiciamiento-criminal/ (visitado el 29.3.2017)

Puede que aplicando los criterios de proporcionalidad tengamos la balanza a favor en cuanto daño causado y daño protegido. Si podemos parar a un delincuente distribuidor de pornografía infantil, aunque se usen imágenes ilícitas, se está previniendo y evitando un daño posterior que es positivo para la sociedad, pero el método empleado es, a mi parecer, un método muy incómodo para los cuerpos de seguridad, porque al fin y al cabo, tras esa fotografía hay un niño o niña que en definitiva es el titular del bien jurídico que se intenta proteger. Y por último y a mi parecer más grave, ha de advertirse del poco control final que tenemos sobre estos archivos. Normalmente estos archivos de contenido ilícito suelen pasar de persona en persona y supongo que los agentes no los dejarán a disposición de todo el que lo quiera utilizar, colgándolo en una red pública, pero puede que otra persona que lo haya obtenido sí lo haga. En el momento en el que dicho sujeto comparte este archivo, la policía deja de tener un control efectivo sobre el mismo y se puede multiplicar exponencialmente llegando a muchas más personas no controladas por los agentes.

Al perder el control sobre estos archivos, la lesión al bien jurídico que se evitaba en el caso del tráfico de drogas no se evita aquí y si lo relacionamos con la problemática anterior acerca de la vulnerabilidad de los niños o niñas que puedan salir en la foto, se convierte en un problema realmente alarmante. Se estaría difundiendo una imagen (por no hablar de que el concepto archivo también contiene vídeos), vulnerando los bienes jurídicos de los que figuran en ella para defender precisamente ese bien jurídico. La metáfora que pretendo destacar es que se estaría atacando al fuego con fuego, de modo que en algunos casos podríamos estar creando una lesión mayor de la que estamos protegiendo. Por otro lado y para ver una visión más positiva acerca de esta posibilidad, es cierto que si este "estudio del algoritmo" se utiliza correctamente podremos determinar todos los equipos que han accedido a este archivo y así rastrear todos los posibles criminales que han estado interesados en descargarlo. No me parece la mejor de las justificaciones pero tengo que reconocer que es útil si además la combinamos con la diligencia de registro remoto sobre equipos informáticos que veremos a continuación.

En definitiva creo que será determinante el nivel de proporcionalidad de las acciones. Se deberá tener en cuenta muchas circunstancias subjetivas en el propio caso y a raíz de esas circunstancias, actuar en consecuencia.

Con ello me refiero a que será muy diferente si el agente utiliza imágenes con una difusión muy amplia y que ya estaban circulando por la red con anterioridad de forma más o menos generalizada a si el mismo agente utiliza imágenes recientes que ha incautado de una operación anterior y que tienen muy poco recorrido en la red. La aplicación de este criterio de proporcionalidad quedará pues en manos del agente, es decir, él será el que tendrá que optar por un medio u otro (siempre dentro de los límites de la autorización judicial) para resolver el caso de la manera más eficiente. Esto a su vez trae consecuencias y es que el agente no siempre tendrá los conocimientos jurídicos suficientes para poder tomar decisiones que encajen en nuestro OJ y esta situación se agrava cuando los límites de su actuación son tan difusos como en este caso. Las consecuencias además pueden llegar a ser graves, ya no solo porque se rechazarían las pruebas obtenidas en la investigación, pudiendo generar una absolución aun y sabiendo la culpabilidad de la persona, sino porque, en el peor de los casos, el propio agente puede llegar a incurrir en un ilícito penal. De momento deberemos esperar a ver qué dice el Tribunal Supremo sobre esta actuación y cuáles son los límites que se imponen y cómo se aplica en estos casos el principio de proporcionalidad tan importante en el derecho penal.

5. Diligencias de investigación relacionadas

I. Rastreo Dirección IP

Hablaremos ahora de una diligencia menos novedosa pero mucho más firme y utilizada por la policía judicial para perseguir a los delincuentes que utilizan la red para cometer sus delitos y especialmente relacionada también con el agente encubierto informático. Lo encontramos en el art. 588 ter k) de la Lecrim y se trata de rastrear la dirección de "Internet Protocol" o más conocida como IP[16]. Este mecanismo permite saber el terminal que se ha utilizado para acceder a la red y por lo tanto poder rastrearlo. En sí, dicho proceso no revela la identidad del sujeto que está detrás del equipo, pero sí podemos acudir después al proveedor de internet para ver los datos de la persona que tiene contratada dicha IP.

Dicho así, parece sencillo, pero la IP forma parte del derecho al secreto de las comunicaciones reconocido en la Constitución (art. 18.3 CE) y por lo tanto la regla general es que sería necesario obtener una autorización judicial para poder llevar a cabo dicha investigación. Ahora bien, la jurisprudencia ha venido interviniendo en un amplio debate generado a partir de los programas peer-to-peer o P2P de descarga (tales como Emule o Edonkey). Estos softwares permiten descargar archivos y al mismo tiempo compartirlos con otros usuarios que estén interesados en el mismo archivo. Son muchas las sentencias que han reconocido estos programas como medios para distribuir archivos ilícitos, siendo los más graves los archivos de pornografía infantil. Por ello, además de aplicar una agravante de la conducta por distribución de pornografía infantil (además de la tenencia), estos programas también permiten rastrear la IP del sujeto sin autorización judicial. La clave del razonamiento radica en que al compartir estos archivos, la IP que utilizamos queda al descubierto, siendo posible que otros usuarios puedan verla y por lo tanto se considera que es una información pública, esto es, pierde la consideración que le otorga el artículo 18.3 de la Constitución.

[16] El Internet Protocol o IP es un número único que identifica todos los dispositivos registrados en una red, es decir, cada uno de los dispositivos que conectemos a internet recibirá un número único que se conocerá como IP, ya sea un móvil, una tablet, una videoconsola, o incluso una impresora. Deberemos diferenciar a su vez entre IP estática (siempre que el equipo se registre recibirá la misma secuencia de números) e IP dinámica (el equipo recibirá una secuencia numérica distinta cada vez que acceda a la red).

La STS **680/2010 de 14 julio** RJ\2010\3509 lo expone perfectamente: *"cuando la comunicación a través de la Red se establece mediante un programa P2P, como en el EMULE o EDONKEY, al que puede acceder cualquier usuario de aquélla, el operador asume que muchos de los datos que incorpora a la red pasen a ser de público conocimiento para cualquier usuario de Internet, como, por ejemplo el I.P., es decir, la huella de la entrada al programa, que queda registrada siempre."*

No obstante, la autorización será necesaria cuando no tengamos esta "publicidad" de la IP. En estos casos, la policía deberá dirigirse al ISP[17] y pedirle la información pertinente a su dirección IP. Para poder obtener la expuesta información sí deberá existir una autorización judicial previa. Una vez mostrada la autorización estos proveedores tienen el deber de proporcionar a la policía la dirección IP y los datos de la persona que la contrató, por lo que generalmente conoceremos la identidad y dirección física. En realidad esta autorización es necesaria porque consideramos la IP como un dato personal, pero lo cierto es que esta concepción también ha generado bastante debate doctrinal. Sin embargo la jurisprudencia del Tribunal Supremo deja clara la configuración de las IPs como datos personales en cuanto son capaces de identificar el equipo con el que se ha trabajado y a partir de ahí podemos llegar al usuario que hay detrás. Concretamente la Sentencia nº 16/2014[18] nos hace un buen resumen de este argumento y cita además otras sentencias en el mismo sentido: *"El carácter de la dirección IP como dato personal ha sido reconocido por la jurisprudencia de esta Sala en numerosas sentencias (SSTS 249/2008, 20 de mayo ; 236/2008, 9 de mayo ; 680/2010, 14 de julio y 292/2008, 28 de mayo), bien entendido que las claves identificativas IPs no concretan a la persona del usuario, sino sólo el ordenador que se ha usado, lo que hace necesario para poder llegar al ulterior conocimiento del número de teléfono y titular del contrato la posterior autorización judicial."*

Sin embargo, parece que la cuestión no está del todo cerrada de suerte que muy recientemente se ha planteado una cuestión parecida al Tribunal de Justicia a raíz de las dudas que surgieron al respecto por parte del Tribunal Supremo Alemán[19].

[17] Proveedor de servicios de internet
[18] STS núm. 16/2014 de 30 enero (RJ\2014\939)
[19] Sentencia del Tribunal de Justicia (Sala Segunda) de 19 de octubre de 2016 (petición de decisión prejudicial planteada por el Bundesgerichtshof — Alemania) — Patrick Breyer / Bundesrepublik Deutschland (Asunto C-582/14)

En las conclusiones redactadas por el abogado general Sr. Campos Sánchez-Bordona se intenta arrojar luz sobre la consideración de las IPs dinámicas como dato personal para las propias compañías proveedoras de servicios, haciendo alusión a la Directiva 95/46 relativa a la protección de estos datos personales. El Tribunal de Justicia acaba llegando a la misma conclusión que el Tribunal Supremo, afirmando que la dirección IP es un dato de carácter personal y que por tanto la compañía que ofrece los servicios sólo podrá acceder a dicha información (sin el consentimiento del usuario) cuando sea estrictamente necesario para la facturación de los servicios contratados.

Por último me parece importante añadir el serio problema práctico que plantea esta medida. Si bien es cierto que en la modalidad que estamos examinando no es tan frecuente, muchos delitos informáticos son cometidos a través de redes públicas. Las redes públicas o abiertas tienen un difícil rastreo puesto que pueden tener decenas o cientos de conexiones simultáneas (véase un aeropuerto, biblioteca o cibercafé). En estos casos es extremadamente complicado poder distinguir entre los distintos terminales que se han conectado a la red y por consiguiente no podremos individualizar al sujeto que nos interesa.

II. Registro remoto sobre equipos informáticos

Viendo a fondo la figura del agente encubierto informático, es imposible no añadir esta nueva diligencia comprendida en el art. 588 septies de la Lecrim que también se incorporó con la reforma del 2015 que hemos estudiado: el registro remoto sobre equipos informáticos. Una figura controvertida, polémica y muy innovadora que se presenta como una medida más para equiparar las herramientas informáticas policiales a las que utilizan los delincuentes. La medida en cuestión permite instalar un malware[20] en un equipo informático de la persona investigada.

[20] se conocen comúnmente como virus y al que se refiere la ley se le conoce como troyanos y además es interesante la connotación negativa que contiene la palabra malware: "malicious software" puesto que es un programa informático dedicado a fines ilícitos o malignos en sus orígenes.

Obviamente, como en todas las diligencias que restringen los derechos de los investigados, esta requiere una autorización judicial. La autorización judicial tendrá a su vez diferentes límites:

1. Solo se podrá aplicar en los delitos que cumplan ciertas características
    a. Los delitos cometidos en el seno de una organización criminal
    b. Delitos de terrorismo
    c. Delitos cometidos contra menores o personas con capacidad modificada judicialmente
    d. Delitos contra la Constitución, de traición y relativos a la defensa nacional
    e. Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.
2. En la autorización habrán de especificarse los equipos que se vayan a intervenir y el alcance de esta intromisión, así como de los agentes que realizarán y el software que utilizarán.
3. La medida tendrá una duración de 1 mes que se podrá prorrogar dos veces por el mismo periodo, es decir, tres meses como máximo.

Como vemos, se trata de unos límites bastante estrictos, sobretodo el límite temporal, convirtiéndose en la medida más restrictiva en cuanto a duración en el tiempo de toda la Lecrim.

Esto nos da a entender que el legislador es consciente de todo lo que puede llegar a significar una manipulación de un equipo informático mediante un malware. En manos de un experto, un troyano puede facilitar el acceso a cualquier parte de nuestro ordenador, smartphone o tablet añadiendo la posibilidad no solo de ver el contenido de los archivos que tengamos almacenados sino de ejecutar cualquier aplicación, acceder a la cámara del dispositivo (incluso registrar lo captado por la misma), hacer capturas de pantalla, ver en todo momento qué está haciendo el sujeto en el dispositivo e incluso acceder a las contraseñas que el usuario pueda tener para cualquier tipo de cuentas privadas de correo, redes sociales, nubes virtuales de archivos etc[21].

[21] Realmente es difícil, según los expertos en la materia, llegar a este nivel de intrusión con un malware, pero en definitiva es posible.

Es necesario añadir que el ordenamiento jurídico español se ha convertido en una especie de pionero en aplicar esta diligencia, como mínimo a nivel europeo[22]. Solo tenemos el ejemplo de Alemania pero en este caso sólo se utiliza para los delitos relacionados con el terrorismo por lo cual no se utiliza demasiado. Parece que nos hemos puesto a la delantera en cuanto a la investigación cibernética y a primera vista puede parecer muy positivo, pero esto también significa que no hay referentes de cómo se ha utilizado esta medida y de momento los límites con los que podemos trabajar son prácticamente inexistentes en la legislación, lo que significa que esta medida tiene muchas posibilidades de ser considerada como una medida que se ha extralimitado en sus funciones. Las partes que puedan pedir la utilización de dicha diligencia pueden verse privadas de las pruebas que deriven de ella por ser inválidas ya que la ley no especifica ningún modus operandi ni nada que ofrezca un poco de luz sobre lo que está permitido y lo que no.

Por otro lado, como hemos visto en la ley, hay un apartado que no parece encajar en la lista de delitos que podemos investigar: Todo delito cometido a través de cualquier medio informático. Parece ser un grupo demasiado abierto para una medida tan intrusiva que choca con el carácter restrictivo de la ley. La doctrina ha sido muy dura con este apartado y resulta ser un punto débil de la misma de suerte que permite perseguir conductas delictivas que no revisten una especial gravedad simplemente porque se ha utilizado un medio informático para cometerlas.

Obviamente tenemos el principio de proporcionalidad para evitar abusos y así proteger la mínima intervención propia del derecho penal, pero si la ley permite expresamente que se persigan esta clase de delitos con una redacción manifiestamente abierta parece que esté justificando la proporcionalidad y que por lo tanto no se tenga en consideración la gravedad del delito. Para ello creo que habrá que esperar a la jurisprudencia y que se manifieste sobre todas estas dudas. Es interesante a su vez fijarnos en el anteproyecto de reforma para con esta medida, donde se establecía que todos los delitos castigados con más de tres años podían ser objeto de investigación mediante el registro remoto.

[22] No tengo conocimiento de ningún otro país utilice esta medida, pero tampoco puedo estar seguro que no la podemos encontrar en ningún otro ordenamiento jurídico del mundo.

Como podemos ver este requisito fue apartado y desechado y actualmente no figura en el redactado final, pero ya se vislumbra la orientación del legislador. Según entiendo, parece que el legislador tenga algún conocimiento sobre las posibilidades del "troyano" pero no da la sensación de que éste le dé demasiada importancia, aunque luego ponga un límite temporal tan estricto. Por un lado parece que intente delimitarla muchísimo temporalmente debido a su intrusión en los derechos fundamentales, mientras que por otro lado deja un gran margen de actuación en cuanto a los delitos que pueden ser perseguidos por la misma.

Ahora bien, como he dicho al inicio del análisis, esta pienso que ésta diligencia va totalmente ligada al agente encubierto online puesto que el agente tiene la capacidad de transferir archivos como hemos visto en el apartado propio de las funciones del agente encubierto online y con estos archivos puede infectar los equipos informáticos donde sean descargados y así acceder a todo el contenido que pueda ser relevante para el caso.

Una vez se ha descargado el archivo en el equipo del investigado (podría ser un ordenador, una tablet o incluso un smartphone) tendremos acceso, suponiendo que lo permita la propia diligencia, a todo lo que queramos de ese equipo. Aunque en este punto creo importante destacar que al fin y al cabo este malware se puede detectar y frenar por los distintos programas conocidos como antivirus. El proceso para crear un malware de este tipo es muy técnico y no entraremos en profundidad, pero sí hay que decir que el equipo técnico policial deberá estar actualizando continuamente estos malwares para que sean indetectables o al menos muy difíciles de detectar. Si esta faena no se hace bien, no solo no podremos sacar información del sujeto sino que también se puede llegar a revelar las intenciones de, en este caso, el agente encubierto y complicar mucho la investigación.

Con todo y con eso, esta medida puede llegar a funcionar en muchos investigados que no sean expertos o técnicos en la materia informática e infectar su equipo sin demasiados problemas. A partir de aquí además podremos desviar esta diligencia hacia otras igualmente interesantes como la intervención de comunicaciones telemáticas, el rastreo de la IP entre otras que veremos más adelante en profundidad.

Aun así está por ver la efectividad de esta medida y su encaje en la legalidad así como los límites que definirá la jurisprudencia. De momento la doctrina la trata con mucho cuidado y es consciente del peligro que supone. Muchos técnicos informáticos reconocidos han opinado también sobre esta medida (muchos de ellos se auto denominan a sí mismos como hackers) y en general no la consideran reprobable siempre que se use con las garantías adecuadas de proporcionalidad y de mínima intervención.

Es muy fácil (y además el redactado de la ley deja la posibilidad abierta) que esta medida se desvíe hacía una función más espía de la que debería alejándose de casos graves como los tratados hasta ahora y se convierta en una herramienta para sacar información de gente poderosa, pero por el momento no adelantemos acontecimientos.

Lo que es indudable es la extrema funcionalidad que tiene esta medida si se ejecuta correctamente, ya no solo a nivel probatorio contra el investigado sino también para descubrir nuevos delitos. El agente encubierto que esté efectuando la investigación podrá ver en los círculos y chats en los que se mueve el supuesto delincuente y a partir de ahí abrir una ramificación de páginas web peligrosas y delictivas que están operando continuamente.

El mundo conocido como deepweb[23] es extremadamente denso y difícil de controlar, son dominios fuera del alcance de Google y no tienen porqué ser ilegales, pero el problema es que si no sabemos la dirección o link de dichos lugares no podemos acceder a los mismos. Por ello si podemos introducirnos en las visitas que ha efectuado el sospechoso podremos encontrar un gran abanico de paginas relacionadas con el delito y conseguir más información para luchar contra ellas. A través de su historial (algo que no debería dar problemas de legalidad para acceder) rastrearemos a otros posibles delincuentes y así frenar de un modo mucho más eficaz delitos tan deleznables como la pederastia o pornografía infantil.

[23] Ver nota al pie 10ª

Generalmente cuando un sujeto de estas características accede a estos registros, no accede a un solo chat y en muchos de ellos obtendrá respuestas de otros sujetos con su misma condición los cuales a su vez visitan otros tantos chats. Por lo tanto, con el registro remoto sobre equipos informáticos podríamos investigar, además del delito inicial, los posibles delitos conexos que se estén llevando a cabo. Si por ejemplo, una banda yihadista se dedica al tráfico de armas o de estupefacientes se podrían descubrir todos los delitos utilizando sólo esta medida.

Con este método podemos ampliar exponencialmente el número de lugares peligrosos en la red e investigar a todos los participantes que encontremos en ellas para evitar que lleven a cabo los delitos que se proponen. Bajo mi punto de vista, creo que es totalmente imposible controlar todos estos lugares y chats, puesto que el número de estas páginas es casi infinito y no sólo eso sino que además crecen sin ningún tipo de control. Pero por otro lado sí que pienso que al evitar la producción de estos delitos, estaremos haciendo una gran función social ya que las consecuencias de cada uno de ellos puede ser devastadora (sobre todo cuando hablamos de terrorismo). Para finalizar este apartado, veremos dos técnicas doctrinales que podrían dar cabida a esta diligencia e intentar salvar las pruebas obtenidas. Ciertamente no sabemos los límites prácticos que pueda tener esta medida y en consecuencia las pruebas obtenidas podrían verse afectadas y anuladas por haber infringido los derechos fundamentales del investigado.

Como decía, para ello podríamos utilizar dos técnicas doctrinales ya asentadas en nuestro ordenamiento jurídico intentando así romper la teoría del fruto del árbol envenenado:

- Eficacia refleja de la prueba prohibida: generalmente se ha venido usando para las escuchas telefónicas. Lo que propone esta técnica es dar como válidas las diligencias efectuadas a raíz de una diligencia anterior aunque esta no estuviera suficientemente motivada[24] siempre que los agentes hubieran actuado de buena fe. Si utilizamos el mismo criterio con el registro remoto sobre equipos informáticos (figura parecida a las intervenciones telefónicas), podríamos salvar las diligencias que se hicieran a raíz de la investigación inicial, permitiendo un pequeño margen de actuación en una medida desconocida actualmente.

[24] Por ejemplo: Se hace una intervención telefónica con una autorización poco motivada que resultará inválida, pero a partir de esas escuchas se descubre el posible delito y se efectúa un registro domiciliario con todas las garantías. Este registro no se vería afectado por la nulidad de la primera diligencia.

- Descubrimiento inevitable: Esta teoría permite mantener la validez de las pruebas conocidas a raíz de una prueba ilícitamente obtenida siempre que ese descubrimiento se fuera a producir en un futuro sin necesidad de la primera prueba (la ilícita). La sentencia del Tribunal Supremo 885/2002 de 21 mayo[25] lo expone francamente bien: *"cuando la experiencia indica que las circunstancias hubieran llevado necesariamente al mismo resultado, no es posible vincular causalmente la segunda prueba a la anterior, pues en tales casos faltará la llamada, en la terminología del Tribunal Constitucional, «conexión de antijuridicidad», que, en realidad presupone, en todos los casos, una conexión causal."*

[25] STS num. 885/2002 de 21 mayo RJ\2002\7411

7. Cadena de custodia en la prueba informática

Una vez hemos determinado todas las funciones y actuaciones del agente encubierto online, nos centraremos en algo imprescindible para que todo lo recopilado durante la instrucción sirva como prueba en el juicio oral: la Cadena de custodia.

La Cadena de custodia trata de asegurar que la prueba que se ha recogido durante la fase de instrucción sea la misma que se presenta ante el juicio oral y que por tanto mantenga la fidelidad y evitar así que se manipule o se transforme. En definitiva de lo que se trata es de mantener la integridad que tenía cuando fue tomada y que no pueda alegarse ninguna alteración en la misma. Generalmente se suele dividir la cadena de custodia en 4 fases:

1. Extracción de la prueba
2. Preservación y embalaje de la prueba
3. Transporte o traslado seguro de la prueba
4. Traspaso seguro de la prueba, al laboratorio u organismo competente que la reclame.

Como podemos ver estas fases responden a pruebas físicas, pruebas que de las que tenemos algo que embalar, transportar y en definitiva asegurar. Las pruebas recogidas por un agente dedicado a descubrir delitos cometidos a través de las redes no suelen coincidir con estas características y por tanto hay que adaptar un nuevo sistema para los archivos digitales.

Seguiremos para ello la visión del perito informático José Aurelio García[26], experto en la materia. Francamente lo expone muy claramente y de forma ordenada en su página web de la que sacaremos gran parte de la información.

[26] AURELIO GARCÍA, José, "La cadena de custodia aplicada a la informática - I" http://www.informaticoforense.eu/la-cadena-de-custodia-aplicada-a-la-informatica-i/ (visitado el 8.4.2017)
AURELIO GARCÍA, José, "La cadena de custodia aplicada a la informática - II" http://www.informaticoforense.eu/la-cadena-de-custodia-aplicada-a-la-informatica-ii/ (visitado el 8.4.2017)

Siguiendo el criterio de José Aurelio García la cadena de custodia debería dividirse en:

1. Identificar: Primeramente deberemos describir el objeto incautado si es que se incauta algún objeto, ya sea físico o virtual. Como bien dice Aurelio García en su blog, si obtenemos un disco duro, tendremos que anotar el modelo y el número de serie del mismo (entre otras características que puedan ser relevantes) para poder diferenciarlo de otros discos duros que podamos tener de otras investigaciones. Es importante destacar que las copias que obtengamos también estar debidamente identificadas.

2. Preservar: Se trata de conservar la prueba original a modo de garantía para su validez en el juicio posterior. Como bien hemos dicho el formato digital nos permite obtener infinitas copias con total libertad. Esto nos permite trabajar con dichas copias y dejar la fuente original guardada y sellada de modo que no se pueda alegar manipulación en la misma.

3. Analizar: Se trata del análisis de la prueba. En cierto modo el análisis informático es más amable porque permite trabajar sin miedo a perder las pruebas de modo que si alguna se corrompe o se pierde, siempre podemos acudir a la prueba original y volver a empezar de cero.

4. Presentar: De poco servirá el análisis si no genera un resultado a modo de informe. Me parece interesante la idea destacada por Aurelio García acerca de la forma de presentación de este informe. El lenguaje informático suele resultar bastante extraño para todos aquellos que no tienen relación con el mismo, esto es, usa muchas palabras abreviadas, siglas o incluso palabras técnicas en inglés que son difícilmente entendibles para alguien que no está introducido en la materia. De este modo será necesario adecuar el lenguaje para que el juez entienda lo que está leyendo y pueda dictar un fallo con pleno entendimiento de las pruebas efectuadas por el perito informático.

Además para hacer un buen análisis de la cadena de custodia sobre estas evidencias digitales será necesario marcar una distinción entre tres tipos de archivos[27]:

1. Archivos estáticos: los archivos estáticos serán aquellos que permanecen independientemente del medio donde se encuentren. Cualquier documento, archivo de imagen, mails u otros archivos similares nos dan una idea de a qué nos referimos. Estos archivos permiten obtener copias idénticas, es decir, podemos clonar el contenido de estas tantas veces como queramos y serán igual de válidas que el archivo original. Por ejemplo en aquellos casos en los que se incaute un disco duro, podremos clonar todo su contenido a otro disco duro y trabajar con todos estos nuevos archivos clonados sin problema, teniendo el disco duro original totalmente sellado o almacenado. Además estas copias amplían el margen de error, de modo que si por algún motivo un archivo resulta dañado o borrado, siempre podremos hacer otra copia con una fidelidad del 100%, incluso permitiendo generar copias de las copias y que estas tengan validez total.
2. Archivos volátiles: Son aquellos datos que se pierden al desconectar el dispositivo de la corriente. Esta consideración resulta inconcebible en una prueba física y por lo tanto hay que tomar medidas especiales de aseguramiento. Por ejemplo puede ser interesante ver qué programas está ejecutando el sujeto en un momento concreto, pero el problema es que en cuanto ese equipo se apague o simplemente cierre el programa no podremos acceder a dicha información. Creo que esto tiene especial relevancia con la medida de registro remoto sobre equipos informáticos, de suerte que podremos obtener pruebas basadas en estos archivos volátiles, porque podemos ver lo que el sujeto hace a tiempo real. A partir de aquí y para no perder dichas pruebas hay diferentes métodos, como hacer capturas de imagen, de vídeo, describir los hechos en un registro o cualquier proceso que trate de convertir estos archivos volátiles en archivos estáticos. Lo que es importante remarcar es que no tiene sentido incautar por ejemplo una memoria RAM (donde tienen lugar todos estos procesos) puesto que al

[27] PERONA JÁTIVA, Enrique, *Análisis Forense. Cadena de Custodia de la evidencia digital* https://www.securityartwork.es/2016/02/10/analisis-forense-cadena-de-custodia-de-la-evidencia-digital/ (visitado el 8/4/2017)

desconectarla de la fuente de alimentación estos datos se perderán, es decir, los métodos convencionales no nos servirán para este tipo de archivos.

3. Archivos en tránsito: Aquellos archivos virtuales que tampoco permanecen en un lugar almacenados sino que son transitorios. Generalmente son datos que se generan, viajan a través de la red y se destruyen cuando han cumplido su función. Generalmente suelen órdenes producidas por distintos programas en la red o peticiones de información como por ejemplo cuando entramos en una página web con registro, esta necesitará comprobar si efectivamente estamos registrados comprobando la base de datos. Esa orden, normalmente, quedará anotada en un Log informático por lo que no es del todo volátil. Aun así la orden que permite acceder sí será transitoria e incluso, combinando esto con un spyware[28] podremos ver cuándo se efectúan y cuál es la respuesta.

[28] Utilizando la técnica del registro remoto sobre equipos informáticos.

8. Conclusiones

Después de haber redactado todo el trabajo considero que estoy en condiciones de dar una visión más crítica y opinión personal del agente encubierto online y sus distintas funciones, así como de las diligencias relacionadas con éste que hemos visto en el trabajo.

Empecemos por el principio. La figura del agente encubierto informático era una actualización totalmente necesaria para el agente encubierto ordinario, además la palabra actualización le queda perfecta en este caso. Hemos visto en el trabajo cómo en el año 2007 ya era reconocida la figura estudiada aunque no la trataban como una especialidad, simplemente era un agente encubierto ordinario llevando a cabo su labor en la red. Con esto quiero decir que era una evolución natural de la técnica policial originaria, de suerte que se permite a la policía judicial adaptarse a las nuevas formas de delincuencia, ofrecer así una mejor investigación y llegar de esta manera al objetivo final: encontrar y demostrar la verdad en el comportamiento del investigado. Es cierto que la reforma está aún en una fase temprana y que en mi opinión está muy indefinida en cuánto a límites, pero es cuestión de tiempo que estos asuntos lleguen al Tribunal Supremo y que este se encargue de resolver y acotar las funciones que puede llevar a cabo un agente encubierto informático.

Comparto mi punto de vista con el del ya citado Fiscal Javier Ignacio Zaragoza Tejada de que no será necesario el requisito de organización criminal para poder perseguir delitos con la figura del agente encubierto online, puesto que era uno de los principales problemas en nuestra Lecrim sin reformar. De este modo no necesitaremos argumentos a mi parecer bastante forzados del Tribunal Supremo para poder considerar como válidas las pruebas obtenidas por el agente. Creo que no tiene sentido que este requisito siga en pie con esta figura ya que los delitos que se cometen a través de la red difícilmente podrán encajarse en esta consideración, pero también considero que es trabajo del legislador dejarlo claro y bajo mi punto de vista, no lo hace.

Esta me parece por lo tanto una de las lagunas más importantes a nivel legal y la que más transcendencia tendría en la investigación. Como he ido señalando a lo largo del trabajo, el agente encubierto online me parece imprescindible de acuerdo con los tiempos en los que vivimos.

La ley intenta actualizar los sistemas de investigación que tiene la policía a su alcance y la idea es muy útil y positiva, pero no acaba de estar definida. La redacción del apartado es muy escaso y poco claro, dejando grandes dudas que no deberían existir, ya no solo porque crea inseguridad jurídica sino porque la actuación de los cuerpos de seguridad queda vinculada a una posible interpretación de la ley llevada a cabo por un Juez de instrucción. Un posible error en la interpretación podría generar la destrucción de una investigación que ha costado mucho dinero, tiempo y esfuerzo.

Aun así he de destacar que la labor llevada a cabo resulta muy efectiva en la lucha contra el crimen. Puede ser descorazonador pensar que tal vez sea imposible frenar todos los delitos que se cometen por internet, pero el simple hecho de frenar un gran número de sujetos hace que valga la pena el esfuerzo dedicado. Durante el trabajo he visto y leído una cantidad importante de sentencias, que aunque después no hayan sido incluidas por no tener relevancia para el mismo, describen unos comportamientos llevados a cabo por el imputado de lo más escabrosos y que gracias a esta función del agente encubierto online han podido pararlos. Por desgracia es innegable que el anonimato que opera en internet genera impunidad, sobretodo porque no podemos controlar todo lo que se genera en la red, sin embargo estoy seguro que la reforma de la ley junto con la labor de los cuerpos de seguridad permitirán combatir contra estos delitos con una eficacia mayor.

Distinta cuestión es la problemática dirigida a las dos diligencias que creo que tienen más relación con el agente encubierto. La consideración de la IP como dato privado y el debate que ha generado me ha parecido muy interesante. Buscando información, me ha llamado la atención que en la rama del derecho administrativo un número de teléfono no es considerado como un dato personal, pero sin embargo la IP sí. No podemos identificar a nadie con una dirección IP, ni siquiera podemos asegurar que esa dirección esté asociada a un solo usuario ya que podemos identificar el terminal mediante el cual se accede pero en ningún caso podemos identificar a la persona que hay detrás. Aún así, en el proceso penal, al menos, se ha llegado a la conclusión que yo creo más acertada, es decir, se considera dato personal cuando tengamos otros datos para identificar a la persona que está detrás de ese código numérico.

Por otro lado tenemos el registro remoto sobre equipos informáticos. Tengo que reconocer que personalmente me fascina esta diligencia y las opciones que genera. Pero ciertamente nos encontramos ante un vacío legal enorme. Durante la redacción del trabajo he intentado extraer información tanto de manuales, como estudios realizados por técnicos o incluso tuve la oportunidad de hablar directamente con un Fiscal con un resultado idéntico en todos los casos: no parece que nadie tenga muy claro en qué consiste esta medida.

Muchas de las explicaciones que he encontrado conllevan al mismo punto: "la policía puede introducir un troyano en tu ordenador, tablet o móvil." Hasta ahí parece todo bastante claro, pero ¿qué ocurre a continuación? Consultando diversas informaciones llego a la conclusión de que un troyano puede hacer de todo en un ordenador ajeno siempre que la persona que lo utiliza sepa cómo hacerlo. No creo que la ley ampare todo este abanico de intromisiones pero por otro lado tampoco creo que la ley introduzca esta medida tan intrusiva, otorgándole un tiempo límite tan estricto y la destine a descubrir archivos que el sujeto pueda tener en el equipo investigado cuando se puede llevar a cabo una incautación del disco duro (entre otras medidas) generando un resultado muy similar. Se me ocurre un símil con el registro domiciliario para responder a esta cuestión, pero es un razonamiento totalmente personal. Cuando accedemos a la vivienda de un sujeto, aunque tengamos la autorización judicial para el propio registro, no podremos acceder a la caja fuerte de este, ni tan siquiera abrir la correspondencia del mismo sin la correspondiente autorización judicial expresa para ello, o una ampliación de la autorización inicial[29].

Imagino que con esta medida ocurrirá algo parecido, de modo que no podremos acceder por ejemplo al correo electrónico del investigado (protegido con contraseña) o encender la webcam de su ordenador para gravar lo que está pasando en la habitación donde esté alojado aunque tengamos una autorización para registrar remotamente su equipo.

Para ello deberemos fijarnos en la propia redacción de la medida y es que en todo momento nos habla de registro, con lo que debo suponer que solo podremos "registrar" su equipo.

[29] De acuerdo con el artículo 588 sexies Lecrim.

Siendo este el razonamiento lógico que hago personalmente, no entiendo entonces la diferencia señalada anteriormente con la medida de registro sobre dispositivos de almacenamiento masivo.

Además tampoco entendería entonces la gran diferencia de requisitos que hay entre las dos, siendo el registro remoto una de las diligencias que más duramente cierra la ley frente a los pocos requisitos que encontramos ante el registro físico sobre dispositivos de almacenamiento masivo. Entiendo que en el registro remoto existe ocultación por parte de la policía y que por lo tanto deba ser más duro pero aun así no me parece motivo suficiente. Verdaderamente tengo mucha curiosidad por saber a qué conclusión llega el Tribunal Supremo y ver los límites que se imponen a dicha medida.

Por último queda por hablar de la cadena de custodia en cuanto a archivos informáticos. Me parece indudable la necesidad de dar una distinta consideración a estos datos puesto que aunque tienen sus ventajas (permiten generar copias infinitas y trabajar más cómodamente), también sus desventajas, ya que muchos datos se pueden perder si no se actúa en el momento preciso o se comete un error en la actuación. Estas características en definitiva pueden acarrear serios problemas a la hora de ser concluyentes para el juicio oral. El principal problema que veo es acerca de los archivos o datos volátiles que ya hemos estudiado. Es imposible presentar ante el juicio una prueba totalmente fiable acerca de estos datos, puesto que en esencia esos mismos datos ya no existen. Los intentos por convertir estos datos en estáticos generan una fuente de prueba a mi parecer poco consistente y fácilmente manipulable.

Muchos de los datos volátiles que se generan podrían ser extremadamente útiles para la investigación y prueba del caso, siendo considerados incluso como prueba de cargo, por lo que es necesario tenerlos en cuenta. Una buena medida para mantener la fiabilidad de los mismos podría ser por ejemplo, utilizar la figura del secretario judicial, garantizando la autenticidad e integridad de la información incautada.

En definitiva, y ya para cerrar este trabajo, tengo grandes expectativas en la evolución del agente encubierto informático y las distintas controversias y debates que hemos visto. Decir también que he aprendido y disfrutado mucho durante la búsqueda de información y redacción del trabajo y que en su totalidad me ha parecido muy interesante.

Veremos depara el futuro para la articulación entre las necesidades de investigación y persecución del delito con pleno respeto a los derechos fundamentales, y una evolución tecnológica cuyo horizonte a medio plazo apenas se puede vislumbrar.

Bibliografía

- AIGE MUT, María Belén, *Las nuevas diligencias de investigación tecnológica Volumen II* Boletín de la Academia de Jurisprudencia y Legislación de las Illes Balears, 2017. (descargado el 14/2/2017)

- ARMENTA DEU, Teresa, *Lecciones de Derecho procesal penal. Octava edición*. Madrid, Editorial Marcial Pons, 2015
- De URBANO CASTRILLO, Eduardo, *Los delitos informáticos tras la reforma del CP de 2010.* Revista Aranzadi Doctrinal num.9/2011 parte Estudio Editorial Aranzadi, S.A.U., Cizur Menor. 2011. (descargado el 7/2/2017)
- GUTIÉRREZ ROMERO, Francisco Manuel, *Algunas claves de la «reforma de la Ley de Enjuiciamiento Criminal»*. Revista Aranzadi Doctrinal num.2/2016 parte Comentario. Editorial Aranzadi, S.A.U., Cizur Menor. 2016. (descargado el 7/2/2017)
- JAÉN VALLEJO, Manuel; PERRINO PÉREZ, Ángel Luis, *La reforma procesal penal de 2015* 1ª Edición. Editorial Dykinson, 2015
- LÓPEZ-BARAJAS PEREA, Inmaculada, *La prueba ilícitamente obtenida y su eficacia refleja.* Actualidad Jurídica Aranzadi num.708/2006 parte Comentario Editorial Aranzadi, S.A.U., Cizur Menor. 2006. (descargado el 29/4/2017)
- ORTIZ PRADILLO, Juan Carlos, *La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación.* Fundación Alternativas 2013 (descargado el 14/2/2017)
- RAMOS MÉNDEZ, Francisco, *Enjuiciamiento criminal: Duodécima lectura constitucional. Duodécima Edición.* Barcelona, Editorial Atelier Libros Jurídicos, 2016
- SANCHÍS CRESPO, Carolina, *Fraude electrónico: su gestión Penal y Civil*. Valencia. Editorial Tirant lo Blanch, 2015.
- ZARAGOZA TEJADA, Javier Ignacio, *El agente encubierto online: la última frontera de la investigación penal.* Revista Aranzadi Doctrinal num.1/2017 parte Tribuna. Editorial Aranzadi, S.A.U., Cizur Menor. 2017. (descargado el 7/2/2017)
- ZARAGOZA TEJADA, Javier Ignacio, *La investigación de la dirección IP tras la Reforma operada por Ley 13/2015.* Revista Aranzadi Doctrinal num.2/2017 parte Comentario Editorial Aranzadi, S.A.U., Cizur Menor. 2017. (descargado el 7/2/2017)

Webgrafía

- "The Italian Squad, NYPD" *Chronicling America: American Historic Newspapers* digital collection https://www.loc.gov/rr/news/topics/italian.html
- AURELIO GARCÍA, José, "La cadena de custodia aplicada a la informática - I" http://www.informaticoforense.eu/la-cadena-de-custodia-aplicada-a-la-informatica-i/ (visitado el 8.4.2017)
- AURELIO GARCÍA, José, "La cadena de custodia aplicada a la informática - II" http://www.informaticoforense.eu/la-cadena-de-custodia-aplicada-a-la-informatica-ii/ (visitado el 8.4.2017)
- CHAVELI DONET, Eduard, "La protección de datos en la reforma de la Lecrim" http://www.govertis.com/aspectos-tic-eecrim-parte-ii (visitado el 15.4.2017)
- COLOM PLANAS, José Luis, "El difícil equilibrio entre la seguridad de los ciudadanos y su privacidad" http://www.aspectosprofesionales.info/2016/08/el-dificil-equilibrio-entre-la.html (visitado el 4.4.2017)
- DE LA TORRE, Adolfo, "El agente policial virtual encubierto, una nueva medida procesal para perseguir el crimen organizado" https://investigacioncriminal.info/2015/10/31/el-agente-policial-virtual-encubierto-una-nueva-medida-procesal-para-perseguir-el-crimen-organizado/ (visitado el 21.2.2017)
- ÉCIJA BERNAL, Álvaro, "Ciberespacio, Dark Web y Ciberpolicía" http://noticias.juridicas.com/conocimiento/articulos-doctrinales/11763-ciberespacio-dark-web-y-ciberpolicia/ (visitado 28.3.2017)
- FERNÁNDEZ GARCÍA, Emilio, "Las nuevas medidas de investigación tecnológica: luces y sombras en las reformas de la Ley de Enjuiciamiento Criminal de 2015" http://www.abogacia.es/2015/12/16/las-nuevas-medidas-de-investigacion-tecnologica-luces-y-sombras-en-las-reformas-de-la-ley-de-enjuiciamiento-criminal-de-2015/ (visitado 5.4.2017)
- PERONA JÁTIVA, Enrique, *Análisis Forense. Cadena de Custodia de la evidencia digital* https://www.securityartwork.es/2016/02/10/analisis-forense-cadena-de-custodia-de-la-evidencia-digital/ (visitado el 8/4/2017)
- RODRÍGUEZ CARO, María Victoria "La infiltración policial: en el límite del Estado de Derecho. El inminente agente encubierto informático" http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10222-la-

infiltracion-policial:-en-el-limite-del-estado-de-derecho-el-inminente-agente-encubierto-informatico/#_Toc421702515 (visitado el 26.2.2017)

- RUBIO ALAMILLO, Javier, "La Informática en la reforma de la Ley de Enjuiciamiento Criminal" http://peritoinformaticocolegiado.es/la-informatica-en-la-reforma-de-la-ley-de-enjuiciamiento-criminal/ (visitado el 29.3.2017)

Jurisprudencia consultada

Audiencia Nacional

- Sentencia Audiencia Nacional (Sala de lo Penal, Sección 1ª) Sentencia nº 25/2016 de 28 septiembre (ARP\2016\1101)

Audiencia Provincial

- Sentencia Audiencia Provincial de Huelva (Sección 3ª) de 25 de Junio de 2015
- Sentencia Audiencia Provincial de Madrid (Sección 23ª) Sentencia nº 471/2015 de 30 junio (ARP\2015\855)
- Sentencia Audiencia Provincial de Barcelona (Sección 9ª) Sentencia de 27 mayo 2014 (JUR\2014\153208)

Tribunal Constitucional

- Sentencia Tribunal Constitucional Sala Segunda nº 173/2011, de 7 de noviembre de 2011. Recurso de amparo 5928-2009.
- Sentencia Tribunal Constitucional Pleno nº 36/1991 de 14 de febrero de 1991

Tribunal Supremo

- Sentencia Tribunal Supremo (Sala de lo Penal, Sección 1ª) Sentencia nº 253/2015 de 24 abril (RJ\2015\1866)
- Sentencia Tribunal Supremo (Sala de lo Penal, Sección 1ª) Sentencia nº 16/2014 de 30 enero (RJ\2014\939)

- Sentencia Tribunal Supremo (Sala de lo Penal, Sección 1ª) Sentencia nº 680/2010 de 14 julio (RJ\2010\3509)
- Sentencia Tribunal Supremo (Sala de lo Penal, Sección 1ª) Sentencia nº 688/2009 de 18 junio (RJ\2009\5975)
- Sentencia Tribunal Supremo (Sala de lo Penal, Sección 1ª) Sentencia nº 292/2008 de 28 mayo (RJ\2008\3241)
- Sentencia Tribunal Supremo (Sala de lo Penal, Sección 1ª) Sentencia nº 236/2008 de 9 mayo (RJ\2008\4648)
- Sentencia Tribunal Supremo (Sala de lo Penal) Sentencia nº 1444/2004 de 10 diciembre (RJ\2005\879)
- Sentencia Tribunal Supremo (Sala de lo Penal) Sentencia nº 885/2002 de 21 mayo (RJ\2002\7411)
- Sentencia Tribunal Supremo (Sala de lo Penal) Sentencia nº 1672/1992 de 10 julio (RJ\1992\6665)

Tribunal de Justicia Europeo

- Sentencia del Tribunal de Justicia (Sala Segunda) de 19 de octubre de 2016 (petición de decisión prejudicial planteada por el Bundesgerichtshof — Alemania) — Patrick Breyer / Bundesrepublik Deutschland (Asunto C-582/14)

Legislación consultada

- Real decreto de 14 de septiembre de 1882, Ley de Enjuiciamiento Criminal.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- DIRECTIVA 2006/24/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE