Facultad de Ciencias Sociales y Jurídicas de Elche

Grado en Seguridad Pública y Privada

Trabajo Fin de Grado

Año académico 2021-2022

TÍTULO

EL AGENTE ENCUBIERTO INFORMÁTICO

AUTOR

PABLO BALLESTER MARTÍN

TUTORA ACADÉMICA

PALOMA ARRABAL PLATERO

ÍNDICE

RESUMEN

El presente trabajo pretende ser un análisis de la figura del agente encubierto informático, que está regulada en nuestra legislación a través de una modificación de la Ley de Enjuiciamiento Criminal efectuada en el año 2015, como respuesta a la creciente problemática que suponen el uso de las tecnologías en el ámbito de la delincuencia.

Es con esta reforma, que ha habilitado a los funcionarios policiales al uso de una serie de medidas de investigación tecnológica, que el legislador ha pretendido facilitar una infiltración eficaz en la ciberdelincuencia actual, así como salvaguardar los derechos fundamentales del investigado.

Se abordará en este trabajo cuál es el concepto del agente encubierto informático, tomando como su antecesor al agente encubierto físico, y la normativa por la cual ha de regirse, definiendo las características del agente policial que hará uso de la misma, así como los cuerpos policiales competentes en nuestro país y una comparativa con otras figuras presentes en las diferentes investigaciones criminales. Terminando con las actuaciones en las que se justifica su uso, así como con las responsabilidades derivadas de la misma.

PALABRAS CLAVE

Agente encubierto informático; agente encubierto; policía judicial; ciberdelincuencia; agente provocador; confidente; ciberpatrullaje.

ABSTRACT

This work aims to be an analysis of the figure of computer undercover agent, wich is regulated in our legislation through a modification of the Law of Criminal Procedure carried out in 2015, as a response to the growing problem posed by the use of technologies in the field of crime

Its with this reform, which has enabled police officers to use a series of technological investigation measures, that the legislator has tried to facilitate effective infiltration in current cybercrime, as well as safeguard the fundamental rights of the investigated.

It´ll address in this work the concept of the computer undercover agent, taking as its predecessor the physical undercover agent, and the regulations by which it must be governed, defining the characteristics of the police agent who will use it, as well as the bodies competent police in our country and a comparison with other figures present in the different criminal investigations. Ending with the actions in which its use is justified, as well as with the responsibilities derived from it.

KEYWORDS

Computer undercover agent; undercover agent; judicial police; cybercrime; agent provocateur; confident; cyber patrol.

ABREVIATURAS

BCIT: Brigada Central de Investigación Tecnológica

BIT: Brigada de Inf

CCN: Centro Criptológico Nacional

CNI: Centro Nacional de Inteligencia

CP: Código Penal

DDAT: Departamento de Delitos de Alta Tecnología

EDITE: Grupo de Delitos Telemáticos

GDI: Grupo de Delitos Informáticos

GDT: Grupo de Delitos Telemáticos

LECrim: Ley de Enjuiciamiento Criminal

LO: Ley Orgánica

SCDTI: Sección Central de Delitos en Tecnologías de la Información

SECRIM: Servicio de Criminalística

STS: Sentencia Tribunal Supremo

TIC: Tecnologías de la Información y Comunicación

UCIBER: Unidad de Ciberseguridad

UCO: Unidad Central Operativa

UIT: Unidad de Investigación Tecnológica

UTPJ: Unidad Técnica de Policía Judicial

INTRODUCCIÓN

El deseo del hombre por transformar el mundo y mejorar su calidad de vida ha dado lugar a una revolución de las tecnologías, un fenómeno que ha cambiado radicalmente las formas de comunicación y convivencia. Este avance ayuda a crear riqueza y bienestar en un mundo cada vez más globalizado, aunque esta misma influencia tecnológica también puede convertirse en una amenaza.

Todo en nuestro día a día pasa a través de las tecnologías. Nuestras actividades cotidianas se llevan a cabo de manera muy diferente a cómo lo hacían nuestros abuelos y abuelas o padres y madres a nuestra misma edad, y será diferente de las de nuestros hijos e hijas.

Desde que suena el despertador, que ya viene integrado en el dispositivo móvil que llevamos a todas partes, todas las acciones de nuestro día a día pasan por este mismo u otro dispositivo electrónico: leer la prensa, revisar y operar con tu cuenta bancaria, consultar tu correo, el tiempo o el estado del tráfico, seguir las indicaciones en tus trayectos, trabajo, reuniones, el contacto con el colegio de tus hijos, compras de todo tipo, así como comunicarte con tu familia y amigos o compartir tus actividades diarias a través de las redes sociales. Aún cuando quedas a cenar con tus amistades, el pago de la cuenta habitualmente se realiza mediante tu dispositivo móvil, e incluso con moneda virtual.

Si casi todo en nuestra vida tiene repercusión en el medio virtual, es lógico que el delito también se vaya a acontecer allí. Este cambio de las actividades cotidianas genera un desplazamiento de oportunidades delictivas para quienes están dispuestos a trasgredir las normas.

El plano virtual ofrece a quien tiene la intención de delinquir una serie de ventajas, que serán asimismo un inconveniente para su persecución. Estas serán, entre otras, el anonimato, la facilidad de esconderse entre millones de usuarios o el cometer delitos con implicaciones en ubicaciones muy distantes a donde se encuentra el mismo delincuente, creando además vacíos legales o implicaciones de distintas leyes a aplicar dentro de un mismo supuesto delictivo.

Como ciudadanos somos conscientes de la inseguridad que conlleva el uso tan extenso de la red en nuestro día a día. Sin embargo, no nos planteamos el anteponer esa seguridad a la comodidad que nos brinda esta otra realidad y es por ello que resulta necesario contar con unas medidas efectivas de seguridad, que deben comenzar desde el uso responsable de las TIC, así como de unos conocimientos básicos de seguridad, algo que puede sobrepasar nuestros conocimientos.

La sociedad busca sentir que su seguridad no está comprometida cuando hace uso de las tecnologías, por lo que puede esperar un debido control de las mismas por parte de terceros, pero al mismo tiempo, es reticente a la idea de que éstos puedan ver su parte más privada, entendiendo que al acceder a ciertos espacios de nuestros dispositivos puede sobrepasarse alguno de nuestros derechos fundamentales. No queremos que nuestro teléfono sea, por ejemplo, rastreado continuamente, ni que las conversaciones almacenadas en él sean accesibles para cualquiera sin una adecuada justificación.

Es por ello que nuestra normativa se viene enfrentando a un reto nunca antes planteado. Del mismo modo que internet ha supuesto una nueva realidad en nuestras vidas, la dificultad añadida a la capacidad de detección y persecución de los delitos en la red, conlleva que nuestro ordenamiento no pueda quedar al margen de esta nueva delincuencia.

Se vuelve cada vez más necesario un modelo judicial adaptado a la misma, que pueda garantizar una justicia penal eficiente, con el reto encontrar un equilibrio óptimo entre el respeto a los principios por los que se rige nuestro estado de derecho y, a su vez, superando las exigencias y dificultades de la nueva criminalidad.

Es en medio de esta vorágine, tras el análisis a este fenómeno y aprovechando el poder de investigación que nos brindan las nuevas tecnologías, el legislador llega a la conclusión de la necesidad de reforma de nuestra LECrim. Así en 2015 aparece el agente encubierto informático, una figura que no ha sido introducida como tal, sino que es la evolución de la ya legislada con anterioridad, el agente encubierto físico.

En este trabajo estudiaremos este nuevo método de investigación, que pretende dar una solución concreta y efectiva a la problemática de una criminalidad cada vez más protegida y oculta o cerrada al exterior, a través de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

El agente encubierto informático es, por tanto, una figura necesaria para sacar a la luz la actividad delictiva ya existente, así como la posible condena de la misma, que no sería perseguible a través de los medios convencionales de investigación.

Su regulación se ha dado con la habilitación de una serie de medidas de investigación tecnológica que facilitan la utilización de una identidad supuesta y de una infiltración más eficaz entre delincuentes. Esta normativa incluye, por ejemplo, la posibilidad de intercambio o envío de archivos ilícitos por parte del agente policial, así como la de analizar los resultados de los algoritmos, necesarios para identificar eficazmente estos archivos ilícitos.

Para solucionar la problemática que plantea el uso de esta figura por parte de los funcionarios policiales, ya que la misma habrá de traspasar ciertas líneas en lo referente al ámbito privado del investigado, así como sustentarse en el engaño como *modus operandi*, se exige que estas medidas deban regirse, en todo momento y sin excepción, por los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad,

Con el fin de garantizar la concurrencia de dichos principios, se prevé como un requisito imprescindible para ser agente encubierto la pertenencia a la Policía Judicial, así como la voluntariedad del agente. Se requerirá de una autorización judicial previa, que este caso se limitará a la del Juez de Instrucción. Además, será necesaria una constante supervisión y posteriores autorizaciones por parte del mismo. De esta manera quedará legitimada la necesidad de esta figura en cada investigación concreta.

Con la redacción de este trabajo pretendo hacer un estudio de esta figura, centrándome en la faceta de investigación, utilizada en la primera fase de nuestro proceso penal.

En la primera parte profundizaré en las características propias de los agentes que llevan a cabo esta tarea, así como las diferentes instituciones que pueden hacer uso de la misma en nuestro país, haré una comparativa con otras figuras que podemos encontrar en nuestro sistema procesal y, pasando por la definición de la figura antecesora de la misma, determinaré cuales han sido las medidas utilizadas por el legislador para adaptar la misma a las carencias de nuestra época.

En la segunda parte, analizaré los tipos de actuaciones en los que está predispuesto el uso del agente encubierto informático, así como de la responsabilidad derivada del mismo.

Con todo lo expuesto, pretendo valorar cómo nuestra ley se ha adaptado a las exigencias de la criminalidad actual, así como generar una opinión crítica con respecto a los puntos fuertes y débiles.

EPÍGRAFE 1. CONCEPTO, ANTECEDENTES Y NATURALEZA JURÍDICA

En este apartado se pone en contexto la figura del agente encubierto informático, explicando cual es su concepto, el entorno donde se plantea su uso, así como la normativa por la que se regula esta figura y sus diferencias con otras que podemos encontrar en una investigación policial, así como con la figura del agente encubierto físico, tomando a ésta como su antecesora.

1. CONCEPTO

Las tecnologías crecen, a la vez que evolucionan, a un ritmo cada vez mayor[1] y con ellas nacen nuevas modalidades delictivas[2], creando vacíos legales con respecto a las medidas de investigación necesarias para la correcta o efectiva persecución de dichos delitos, y es por ello que se crea la necesidad ante el legislador de regular la figura del agente encubierto informático[3].

Es en la red donde la sociedad actual ha ido evolucionando a pasos agigantados, ya que absolutamente todo pasa a través de ella. Ocio, comunicación, información, vida social, formación, política, salud, trabajo y economía se reúnen en dispositivos que nos acompañan veinticuatro horas al día.

Vivimos expuestos, en mayor o menor medida, ante el resto de los usuarios de las redes, independientemente de nuestros conocimientos específicos sobre seguridad en las

[1] Los indicadores del informe Digital de 2022 realizado por *We Are Social* y *Hootsuite* señala que se ha llegado al 67,1% de usuarios de internet en dispositivos móviles en el mundo, al 62,5% de usuarios de internet y al 58,4% de usuarios activos de redes sociales. En solo diez años, el número de usuarios prácticamente se ha duplicado. Para más datos consultar: https://marketing4ecommerce.net/usuarios-de-internet-mundo/ (Visitado el 12 de marzo de 2.022).

[2] A modo de ejemplo, las nuevas tecnologías han creado nuevos tipos delictivos como serían el sexting, el pishing, ciberbullying, robo de datos, delitos contra la propiedad intelectual, etc.

[3] Así la exposición de motivos de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECRIM que la regula, señala: "La Ley de Enjuiciamiento Criminal no ha podido sustraerse al paso del tiempo. Renovadas formas de delincuencia ligadas al uso de las nuevas tecnologías han puesto de manifiesto la insuficiencia de un cuadro normativo concebido para tiempos bien distintos... Por muy meritorio que haya sido el esfuerzo de jueces y tribunales para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática de nuestro sistema procesal, carencia que tanto la dogmática como instancias supranacionales han recordado".

mismas. Por tanto, no es de extrañar que nuestra vulnerabilidad sea un aliciente hacia quien está decidido a delinquir.
En el momento en que nuestras transacciones económicas, vida social e íntima pasan al plano virtual, estamos dando lugar a oportunidades delictivas en este terreno, que podrán ser llevadas a cabo desde el anonimato y en cualquier lugar del mundo, independientemente de donde se encuentre la potencial víctima.

La figura del Agente Encubierto Informático nace, por lo tanto, de la necesidad de infiltración en la Red de un empleado o funcionario público miembro de la policía judicial que, previa decisión de una autoridad judicial y de manera voluntaria, persiga obtener información sobre prácticas ilícitas y posibles hechos delictivos realizados a través de las nuevas tecnologías[4].

El agente encubierto informático es, sin lugar a dudas, una herramienta necesaria para combatir la delincuencia actual, y esto también debe de definirse claramente, puesto que nada tiene que ver con el tipo de delincuencia reflejada en las leyes anteriores, donde el escenario de la red no era contemplado.

Se trata de una medida concreta de investigación tecnológica, prevista en la LECrim, específicamente en los apartados 6 y 7 del artículo 282bis, que serán expuestos más adelante, mediante la ocultación de la identidad policial del agente de la policía judicial y la integración en la red entre el resto de usuarios, con el fin de ganarse su confianza y así, sin ser detectado, obtener pruebas suficientes sobre los hechos ilícitos que éstos habrían perpetrado[5].

Debido a las características especiales del entorno de la red, donde no siempre es posible separar las actividades lícitas e ilícitas que desarrolla un mismo usuario, serán determinados agentes pertenecientes a la Unidad Orgánica de la Policía Judicial, principalmente pertenecientes a la Policía Nacional y la Guardia Civil, quienes cumplan las funciones especificas de investigación penal en este ámbito.

[4] Concretamente podrán infiltrarse: miembros de la Policía Nacional, miembros de la Guardia Civil y agentes de policías autonómicas, siempre que tengan competencias de Policía Judicial, salvo en investigaciones encubiertas con implicaciones internacionales, al no ser funcionarios de policía a efectos del Convenio Schengen.
[5] ZARAGOZA TEJADA, J.I., "El agente encubierto online: la última frontera de la investigación penal", *Revista Aranzadi Doctrinal*, nº1, 2017, p.198.

El porqué de acotar el uso de esta medida a los agentes integrantes de la Policía Judicial y no a cualquier funcionario perteneciente a los Cuerpos Policiales del Estado, se debe a que las funciones de dicha unidad están regidas por los principios de permanencia, estabilidad, especialización y estricta sujeción o dependencia funcional de jueces, tribunales y Ministerio Fiscal[6]. La regulación de estas unidades se establece el RD 769/1987, de 19 de junio (reformado el 29 de enero de 2.002) y se complementa con los artículos 126 de la CE y 282 de la LECrim.

Ya en el año 2001 el debate social en nuestro país se extiende ante la necesidad de regulación de diversos delitos informáticos, tal y como se reflejada en diferentes editoriales especializadas, donde se habla de la necesidad de definir conceptos como el ciberdelito, así como de la problemática a la hora de tipificar los diferentes delitos informáticos y la necesidad de convenio y creación de tratados internacionales de cooperación y colaboración[7].

Estas carencias normativas no son un hecho aislado en nuestro país. El 23 de noviembre de 2001 es aprobado por el Consejo de Europa el Convenio sobre la Ciberdelincuencia de Budapest, que define la ciberdelincuencia como *"*aquellos actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de los sistemas, redes y datos*"*[8].

En el artículo 1 del citado convenio encontramos los términos de sistema informático, que *"*se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa" y el de datos informático, que dice que "se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función*"*.

[6] Para profundizar en este tema, léase CUADRADO SALINAS, C., "La Policía Judicial", en *Derecho procesal penal* (Coord. FUENTES SORIANO, O.), Tirant lo Blanch, Valencia, 2020, pp.101-111.

[7] MITCHSON, N., URRY. R., "Delitos y abusos en el comercio electrónico". *The IPTS Report*, 2001, nº57, pp. 19-24.

[8] Siendo ratificada esta definición por España en el BOE, núm. 226/2010 de 17 de septiembre de 2010.

Según detallaba MIRÓ LLINARES en el año 2011, en los últimos tiempos, el término cibercrimen se ha venido utilizando por los especialistas en el área a la hora de hablar de los delitos informáticos[9] (careciendo este término de una definición universalmente homogénea o aceptada por todos) con el fin de reflejar o expresar de mejor manera la característica esencial que lo diferencia de otro tipo de delincuencia[10].

El término cibercrimen, en su origen, venía usándose en referencia al término anglosajón *cybercrime*, que nace de la unión el prefijo *cyber*, del término *cyberspace*[11], y el término *crime*. Por tanto, el término cibercrimen englobaría a cualquier tipo de delincuencia relacionada con el uso de las TIC[12].

Al abarcar este término un espacio tan amplio como es la red, podemos englobar dentro de la ciberdelincuencia a todo delito en el que el objeto de la actividad delictiva sean los propios sistemas informáticos o las TIC, siendo los objetivos tanto los dispositivos informáticos (por ejemplo, ataques por virus informáticos o espionaje de sistemas informáticos a empresas o incluso a estados) como los datos (acceso sin autorización a datos, programas o sistemas informáticos, descubrimiento y revelación de secretos registrados en ficheros o soportes informáticos).

También entendemos por ciberdelincuencia a todo tipo de delitos cometidos a través de la red, como podrían ser: las estafas informáticas, la pornografía infantil, el robo de identidad o el ciberacoso.

Teniendo estos tipos de delitos unas características tan específicas, como son el anonimato y la no personación del infractor en el momento de cometerlo, la posibilidad de acceder a multitud de personas a la vez y de diferentes partes del mundo, se crean

[9] MIRÓ LLINARES, F., "La oportunidad criminal en el ciberespacio: aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen." *Revista Electrónica de Ciencia Penal y Criminología.* https://dialnet.unirioja.es/metricas/documentos/ARTREV/4396388, noviembre 2011, pp.2-3.
[10] Véase, por ejemplo, DE LA CUESTA ARZAMENDI, J. L. (DIR.)/DE LA MATA BARRANCO, N. J. (COORD.):Derecho penal informático, Civitas, Cizur Menor, 2010. En nuestro país institucionalmente se prefiere esa denominación para, por ejemplo, la fiscalía delegada en materia de delitos informáticos.
[11] Término creado por el novelista de ciencia ficción William Gibson y su obra Neuromancer, AceBooks, New York, 1984.
[12] Abreviatura de Tecnologías de la Información y la Comunicación.

una serie de ventajas a la hora de poder delinquir, y así consecuentemente, una mayor dificultad en la persecución de dichas actividades[13].

Como señala PÉREZ ARIAS, esta forma de criminalidad no constituye una categoría normativa, ni permite un concepto unívoco, al no estar claramente definida por el legislador español y siendo un término utilizado más que por juristas, por criminólogos y profesionales de la informática y seguridad tecnológica[14].

Estas definiciones tan amplias, a mi parecer, crean una dificultad añadida a la hora de perseguir eficazmente dichos delitos, ya que la ciberdelincuencia como tal, no es una actividad delictiva única, sino toda una serie de actividades ilícitas o ilegales que necesitan de nuevas tecnologías o del ciberespacio para cometerse.

Todo ello sumado a la falta de concienciación sobre seguridad informática, por parte de los usuarios de las mismas, hace que dichas conductas delictivas sean más fáciles de llevar a cabo sin disponer de muchos conocimientos, ya que el propio crimen organizado, con la intención de llevar a cabo ciertos delitos, contrata a ciberdelincuentes especializados en este ámbito donde se requieren conocimientos más específicos[15].

Otro factor a tener en cuenta es la adaptación al cambio por parte de los delincuentes, que en el escenario del avance tecnológico en nuestras vidas, va por delante de nuestra normativa y de las propias fuerzas y cuerpos de seguridad, problema del que se hace eco la ONU, cuando plantea la cuestión de cómo las respuestas de las autoridades deben lograr mantenerse a la par con el ritmo de innovación de la ciberdelincuencia[16].

Por todo lo expuesto, creo necesario adaptar la ley a estas nuevas formas delictivas, mediante una actualización sistemática del Código Penal, con la colaboración de expertos en la materia, abierta a posibles modernizaciones de conceptos y delitos que

[13] MIRÓ LLINARES, F., "La oportunidad criminal…, Op.Cit, pp.1-55.
[14] PÉREZ ARIAS, J., "Cibercriminalidad: hacia la nueva realidad virtual del derecho penal" *Revista Internacional de Doctrina y Jurisprudencia,* España 2021, p.183.
[15] Para profundizar en el estudio del phinsing léase: REY HUIDOBRO, LF., "La estafa informática: relevancia del phising y el pharming", *Diario La Ley, nº7926, 2012.*
[16] ONU (A/CONF.222/12) 13º Congreso de las Naciones Unidas sobre prevención del delito y justicia penal. Celebrado el 2 de febrero de 2015.

sean más acordes a nuestra realidad global, económica y social. Así, se solventaría la necesidad de reiteradas modificaciones, normalmente a posteriori, de la aparición de diferentes modalidades delictivas, tal y como viene siendo lo habitual.

Ante esta realidad, tal y como se extrae del reciente proyecto de Estrategia de Seguridad Nacional 2021, se ha convertido en un tema de principal preocupación para los gobiernos el garantizar la ciberseguridad nacional, dando prioridad a la creación de normativas que estén dirigidas a prevenir, investigar y defender activamente a la misma[17].

Se señala en este proyecto la hiperconectividad, como un rasgo definitorio de la sociedad actual, tanto en actividades públicas, como profesionales y privadas. Remarcando en el mismo que la vía para proteger los derechos y libertades de los ciudadanos, pasa necesariamente por garantizar la seguridad dentro del ciberespacio.

La prioridad de organizaciones y gobiernos será, por tanto, la de proteger el ciberespacio de ciberataques y ciberincidentes, en el ámbito público como el privado, ya que éstos se han visto aumentados en los últimos años.

Se ha elaborado además, una Carta de Derechos Digitales que, si bien no es vinculante, indica la voluntad del legislador de proteger los derechos de la ciudadanía en el entorno virtual, así como reconocer derechos como el de igualdad, de no discriminación y de no exclusión en el ámbito digital[18].

Creo necesario, para entender el papel que va a desempeñar el agente encubierto informático, definir previamente qué tipo de agente policial podrá actuar como tal.

---

[17] La estrategia de seguridad nacional ha sido elaborada bajo la coordinación del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, siendo el Consejo de Seguridad Nacional el órgano responsable del mismo, junto con los departamentos ministeriales, el Centro Nacional de Inteligencia y con la participación de Comunidades y Ciudades Autónomas y expertos en materia de seguridad. Ésta estrategia será revisada cada 5 años, habiéndose adelantado la última revisión tras la reciente crisis acontecida por la pandemia del Covid-19, tal y como se especifica en la misma. Para profundizar en el tema, léase el informe en https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021 (Fecha consulta: 10 de mayo de 2.022).

[18]Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2021/Julio/Noticia-2021-07-15-El-Gobierno-de-Espana-adopta-Carta-Derechos-Digitales.html#.YooBTWBBxUI (Fecha de consulta: 10 de mayo de 2.022).

1.1. AGENTE DE POLICIA JUDICIAL

En el artículo 282 bis de la LECrim, que será detallado más adelante, se indica que para poder actuar como agente encubierto informático, será requisito imprescindible pertenecer a la Policía Judicial.

La unidad de la Policía Judicial, según el artículo 7 del Real decreto 769/1987, de 19 de junio, sobre regulación de la Policía Judicial[19], está integrada por aquellas Unidades Orgánicas previstas en el artículo 30.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. Éstas unidades se formarán con funcionarios de las Fuerzas y Cuerpos de Seguridad del Estado y se regirán por los principios de territorialidad, permanencia, estabilidad, y especialización[20].

Las unidades de la Policía Judicial dependerán asimismo de jueces, tribunales y Ministerio Fiscal. Dado que el proceso penal español se rige por el principio de garantía procesal del acusado, especialmente en lo relativo a los derechos fundamentales, resulta evidente la necesidad de equilibrio entre la investigación de un hecho delictivo y la debida supervisión ante una posible intromisión en dichos derechos.

Responde acertadamente el legislador a esta necesidad, mediante el requerimiento de autorización judicial previa, indispensable para realizar ciertas funciones de policía judicial, y a mi juicio, especialmente, a la hora de actuar como agente encubierto informático.

En el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, se especifica que competerá la función de Policía Judicial, dentro de sus respectivas

[19] Artículo 7 del Real Decreto 769/1987, de 19 de junio, sobre regulación de la Policía Judicial. Actualizado el 29 de enero de 2002.
[20] Como se especifica en el artículo 32 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, dicha especialización será acreditada por una titulación expedida por el Centro de Estudios Judiciales, que constará de dos fases. La primera de ellas, en los centros de formación de las FFCCSE. La segunda, en el centro de Estudios Judiciales.

competencias, a los miembros de Fuerzas y Cuerpos de Seguridad dependientes del Gobierno, las comunidades autónomas o de los entes locales[21].

Las funciones de la Policía Judicial serán las de prevención e investigación de hechos delictivos. Concretamente la averiguación del delito, descubrimiento y aseguramiento del delincuente, según se recoge en el artículo 126 de la Constitución, siempre en los términos establecidos por la ley y bajo la dependencia de las autoridades judiciales.

Su objeto y obligación será la de averiguar los delitos públicos cometidos en su territorio, debiendo practicar las diligencias necesarias para identificar a los delincuentes, así como recoger todas las pruebas del delito para poner a disposición judicial. Así se recoge en el art.282 de la LECrim y en el artículo 549 de la Ley Orgánica 6/1985[22].

El legislador ha previsto a la Policía Judicial las labores de realización de diligencias de prevención o investigación, de forma autónoma, con el artículo 284 de la LECrim, así como las de ejecutar las diligencias de investigación que le sean encomendadas por parte de los jueces de instrucción y del Ministerio Fiscal, según el artículo 287 de la LECrim.

Por lo tanto, centrándonos en el agente encubierto informático, tal como detalla GÓMEZ DE LIAÑO FONSECA-HERRERO cuando hablamos del mismo, estaríamos hablando de agentes pertenecientes a esta unidad, que así lo decidan voluntariamente, complementándose con la acreditación de su formación criminológica, jurídica y psicológica por parte de sus mandos policiales[23].

[21] Artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Añadido por el artículo 125 de la Ley Orgánica 19/2003, de 23 de diciembre.
[22] Artículo 549 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Añadido por el artículo 125 de la Ley Orgánica 19/2003, de 23 de diciembre.
[23] GÓMEZ DE LIAÑO FONSECA HERRERO, M., *Criminalidad organizada y medios extraordinarios de investigación*, Cólex, Madrid 2004, pp.177-178.

Tal como detalla POZO PEREZ, podrán infiltrarse concretamente a nivel estatal, funcionarios del Cuerpo Nacional de Policía y de la Guardia Civil pertenecientes a la Policía Judicial[24].

Por su parte, a la Policía de las Comunidades Autónomas y de las Corporaciones Locales se les atribuye el carácter de colaborador de la Policía Judicial de acuerdo con el artículo 29.2 de la Ley Orgánica 2/1986, como puntualiza CAROU GARCÍA[25]. Así entendemos que, coexistiendo legalmente ambas normativas, puede darse la competencia de Policía Judicial dentro de estos cuerpos, siempre que se respete el criterio de territorialidad y de especialización especificados en el artículo 30.1 de la citada Ley.

Por lo tanto, podrán infiltrarse a nivel autonómico agentes de Policías Autonómicas en sus respectivas comunidades autónomas, cuando les haya sido prevista la competencia de Policía Judicial en sus Estatutos Autonómicos. Estas serían, la Ertzaintza en el País Vasco[26], los Mossos d'Esquadra en Cataluña[27] y la Policía Foral en Navarra[28].

Como límite a la actuación de la Policía Judicial autonómica, nunca podrá producirse su infiltración cuando las implicaciones de la investigación sean de carácter internacional, siendo reconocida esta competencia únicamente a los cuerpos considerados como tal a efectos del Convenio de Shengen. Estos cuerpos serán en España, la Policía Nacional y la Guardia Civil[29].

En cuanto a las policías dependientes de Corporaciones Locales, lamentablemente, queda descartada su infiltración como agente encubierto informático, ya que no se cumple el requisito de especialización y capacitación exigido a estos agentes de la

[24] DEL POZO PÉREZ, M., "El agente encubierto como medio de investigación de la delincuencia organizada den la Ley de Enjuiciamiento Criminal española", *Revista Criterio Jurídico*, vol.6, 2006. p.287.
[25] CAROU GARCÍA, S., "El agente encubierto como instrumento de lucha contra la pornografía infantil en internet" Cuadernos de la Guardia Civil, Revista de Seguridad Pública nº 56, 2018, disponible en https://www.guardiacivil.es/es/institucional/Cuadernos_de_la_Guardia_Civil/index.html , pp.32-34.
[26] Art.17 de su Estatuto Autonómico y arts.112 a 115 Ley 4/1992, de 17 de julio, de la policía Vasca.
[27] Art.13 de su Estatuto Autonómico y arts.13 a 15 de Ley 10/1994, de 11 de julio, sobre la Policía de la Generalitat. Real Decreto 54/2002, de 18 de enero y 191/2002, de 22 de enero y 147/2002 de 28 de mayo.
[28] Art.51 de la Ley 13/1982, de 10 de agosto y el Decreto Foral 213/2002, de 14 de octubre, que aprueba el texto refundido de la Ley Foral de Cuerpos Nacionales de Policía de Navarra.
[29]Acuerdo del 14 julio 1985. Firmada la adhesión de España el 19 de junio de 1990.

Policía Judicial. Por tanto, aun pudiendo iniciar una investigación, su labor como policía judicial es muy limitada, ya que serán los cuerpos policiales con plenas competencias de policía judicial, quienes culminen las labores de investigación, quedando su labor relegada a la figura de agente colaborador.

Además, no podrán ser agentes encubiertos informáticos los agentes de los servicios de inteligencia del Estado[30], si bien podría darse el caso, como veremos más adelante.

Tampoco lo serán los agentes del servicio de vigilancia aduanera, aunque el artículo 2 del acuerdo de adhesión del reino de España al acuerdo Schengen, sí contempla algunas competencias específicas en materia de policía judicial, como serían las relativas al tráfico ilícito de estupefacientes y sustancias psicotrópicas, el tráfico de armas y explosivos o el transporte de residuos tóxicos y nocivos, siempre que cuenten con acuerdos bilaterales apropiados.

Para profundizar en la figura del agente encubierto informático, dentro de las diferentes Policías Judiciales, es necesario tratar cada cuerpo policial por separado, ya que cuentan con unidades específicas en materia de ciberdelicuencia.

Como inciso personal, creo que sería interesante tanto la creación de una especialidad como agente encubierto informático, que requiera de una capacitación suplementaria a la ya adquirida por los agentes de policía judicial, así como una serie de protocolos de cooperación y coordinación entre los diferentes cuerpos, donde compartir información de las investigaciones, ya que la limitación territorial de estas pueden solaparse, debido a la magnitud del ciberespacio.

1.1.1 POLICIA NACIONAL

Es en 1995 cuando, con tan solo unos 40.000 ordenadores conectados a internet en España, se crea el Grupo de Delitos Informáticos, en la Brigada de Delincuencia

[30] Art.4 y 5 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

Económica y Financiera de la Comisaría General de la Policía Judicial[31]. Esto es debido a que ya se producían ataques y vulneraciones de derechos a través de internet, así como estafas bancarias.

En el año 2.000, coincidiendo con la aparición del ADSL, se crea la Unidad de Investigación de la Delincuencia en Tecnologías de la Información, evolucionando en el año 2002 a la actual Brigada de Investigación Tecnológica (BIT).

La BIT depende de la Unidad Central de Investigación Tecnológica (UIT), está estructurada en una Jefatura de Unidad al mando de un Comisario, (de la que dependen directamente dos secciones Operativas, al mando de dos Inspectores Jefes, compuestas por varios Grupos Operativos cada una de ellas) y una Sección Técnica, (con un Inspector al frente y con Grupos Técnicos)[32].

Tal y como nos detalla la Policía Nacional en su propia web, será la UIT (Comisaría General de la Policía Judicial) quien asuma las competencias de investigación y persecución de las actividades delictivas producidas en la red[33].

Dichas actividades delictivas serán las que impliquen el uso de las TIC y el ciberdelito a nivel nacional y transnacional, relacionadas con los delitos de pornografía de menores, contra la libertad sexual, el patrimonio, consumo, la intimidad, el honor, redes sociales, fraudes, propiedad intelectual e industrial y de seguridad lógica.

Esta unidad actuará como Centro de Prevención y Respuesta E-Crime y de ella dependerán la Brigada Central de Investigación Tecnológica (BCIT) y la Brigada Central de Seguridad Informática.

Dichas brigadas se centrarán en obtener pruebas, perseguir a los delincuentes y poner a unas y otros a disposición de las autoridades judiciales.

---

[31] Para profundizar en el tema, léase: La historia de internet en España, disponible en https://blogthinkbig.com/historia-de-internet-en-espana (Fecha de consulta: 10 de abril de 2.021).

[32] DECUMA, Temario Policía Nacional, Escala Básica, TEMA 33 Delitos informáticos. Protección de datos. Especial consideración al derecho a la intimidad. La prueba digital en el proceso penal. El agente encubierto informático.

[33] Información disponible en su web: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial.php (Fecha de consulta: 20 de marzo de 2.022).

Los agentes de esta unidad se caracterizan por la formación continua, la colaboración con instituciones públicas y privadas, así como la participación en foros de cooperación policial internacionales y la colaboración ciudadana.

La BCIT investigará las actividades delictivas relacionadas con la protección de menores, la pornografía infantil, la intimidad, la propiedad intelectual e industrial, las estafas, piratería, ataques cibernéticos, etc[34].

La Brigada Central de Seguridad Informática investigará las actividades delictivas que afecten a la seguridad lógica y a los fraudes en las telecomunicaciones.

1.1.2 GUARDIA CIVIL

El mando de Información, Investigación y Ciberdelincuencia, a cargo de un Teniente General de la Guardia Civil, es el responsable de la Jefatura de Información y la Jefatura de Policía Judicial, para su dirección, impulso y coordinación del servicio[35].

La Jefatura de Información organiza, dirige y gestiona la obtención, recepción, tratamiento, análisis y difusión de la información de interés para el orden y la seguridad pública, así como utiliza operativamente la información relativa al terrorismo nacional e internacional. Tiene al mando un Oficial General de la Guardia Civil.

La Jefatura de la Policía Judicial, organiza y gestiona la investigación y persecución de delitos y faltas, así como desarrolla los servicios de criminalística, identificación, analítica e investigación técnica. Tiene al mando a un Oficial General de la Guardia Civil y colabora con otros cuerpos policiales nacionales y extranjeros.

[34]Información disponible en su web: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php (Fecha de consulta: 20 de marzo de 2.022).
[35] Información disponible en su web: https://www.guardiacivil.es/en/institucional/Conocenos/estructuraorganizacion/orgcentral/mando_investi_inf_ciber/index.html (Fecha de consulta: 14 de abril de 2.022)

De la Jefatura de Policía Judicial dependen la Unidad Central Operativa (UCO), la Unidad Técnica de Policía Judicial (UTPJ) y el Servicio de Criminalística (SECRIM).

La UTPJ realiza asesoramiento técnico al mando de la Jefatura de la Policía Judicial en sus funciones, centraliza la información relativa a delitos de interés, tanto para la acción de mando, como para la operatividad de las unidades de Policía Judicial territoriales, ubicadas en el nivel provincial. Además, está al cargo de la elaboración de normas técnico-operativas, así como de centralizar la gestión e intercambio de información con otros organismos afines a nivel nacional e internacional. También encuadra a efectos administrativos al personal de la Guardia Civil que se encuentra destinado en órganos compartidos con otros cuerpos policiales nacionales e internacionales, como serían Interpol, Europol, Sirene, etc.

El Servicio de Criminalística aplica técnicas y procedimientos científicos especiales, elabora informes periciales y técnicos, así como identifica a personas en sucesos con víctimas múltiples, presta apoyo técnico-operativo y de investigación científica, todo ello de acuerdo a la demanda de Órganos Judiciales y de las Unidades de Investigación.

La UCO investiga y persigue la delincuencia organizada, económica e internacional, colabora, coordina y establece enlaces con otros servicios afines, nacionales e internacionales.

Es dentro de la UCO donde encontramos la unidad actualmente conocida como Grupo de Delitos Telemáticos (G.D.T.), que tiene sus inicios en 1996, con el Grupo de Delitos Informáticos (GDI), ante la necesidad de perseguir eficazmente los delitos informáticos debido al auge y relevancia de los mismos, tal y como informan en la página web de la Guardia Civil[36].

En 1999, para adoptar una terminología más acorde a la realidad de sus actuaciones, esta unidad es denominada Departamento de Delitos de Alta Tecnología (D.D.A.T.) y es en 2003 cuando adopta su actual nombre.

[36] Información disponible en su web: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php (Fecha de consulta: 14 de abril de 2.022).

Ya en sus inicios se especializó a sus agentes con formación informática, pero es en el año 2000, cuando expertos policiales provenientes de la Guardia Civil participan en el Convenio de Ciberdelincuencia del Consejo de Europa. A partir de ese momento se opta por una mayor especialización, estructurando a sus miembros en diferentes áreas específicas como la de pornografía infantil, fraudes y estafas, propiedad intelectual y delitos de hacking.

El G.D.T. es miembro activo de los Grupos de trabajo de Interpol en Europa y Latinoamérica (son los organizadores del Foro Iberoamericano de Encuentro de Ciberpolicías desde 2002), en el Grupo de Europol y en el Foro Internacional del G-8 para el cibercrimen.

A día de hoy, son los Grupos de Delitos Telemáticos (E.D.I.T.E.) quienes se encargan de estas funciones a nivel provincial, estando encuadrados en las Unidades de Policía Judicial de la Guardia Civil.

Estos grupos se encargan de las actividades de prevención, con la detección de delitos informáticos en la red, investigaciones de los diferentes delitos informáticos por propia iniciativa, bajo requerimiento de las autoridades judiciales o a través de las denuncias de los ciudadanos. Además, estos grupos especializados sirven de apoyo a otras investigaciones del resto de Unidades de la Guardia Civil.

1.1.3 POLICÍAS AUTONÓMICAS

En la actualidad, numerosas Comunidades Autónomas cuentan con cuerpos policiales propios, variando su régimen competencial en función de sus estatutos propios. En este sentido, podemos distinguir entre las policías autonómicas con plenas competencias o de competencias restringidas, en materia de Policía Judicial.

Los cuerpos policiales autonómicos con competencias restringidas de Policía Judicial son las Unidades Adscritas[37].

[37] De adscripción de unidades de la Policía Nacional.

Los cuerpos policiales autonómicos con plenas competencias en materia de Policía Judicial son la Ertzaintza en el País Vasco, los Mossos d'Esquadra en Cataluña y la Policía Foral de Navarra, ésta última, si bien contaba con competencias plenas, no las ha asumido hasta hace poco.

La Ertzaintza asume su competencia íntegra en materia de Policía Judicial, mediante su Estatuto de Autonomía[38]. En desarrollo del precepto de protección de personas y bienes, así como del mantenimiento de la seguridad pública, se promulga la L.O. 4/1992, de 17 de julio, de Policía del País Vasco.

Cuando en 1986 se promulga la L.O. de Fuerzas y Cuerpos de Seguridad del Estado, se incluye en la Disposición Final Primera, una cláusula por la que las disposiciones de esta Ley no serán de aplicación a las competencias contenidas en el artículo 17 del Estatuto de Autonomía de las instituciones del País Vasco. Este artículo reconoce la facultad de la Policía Autonómica Vasca en materia de Policía Judicial, bajo vigilancia de la Autoridad Judicial. El desarrollo normativo de la función de Policía Judicial para la Ertzaintza se especifica en la Sección III, Policía Judicial, de la L.O. 4/1992.

Dentro de la Ertzaintza, en la Unidad de Investigación Criminal y Policía Judicial, se ubica la Sección Central de Delitos en Tecnologías de la Información (S.C.D.T.I.), encargada del descubrimiento e investigación de los delitos relacionados con internet y las TICS, así como de prestar apoyo técnico y cobertura a las actuaciones de la Ertzaintza en estas cuestiones, tal y como detallan en su web[39].

Además, debido a que sus agentes cuentan con formación específica en aspectos jurídicos y técnicos, así como amplia experiencia en investigación criminal, se encargan también de la instrucción y diligenciamiento de delitos graves.

Los Mossos d'Esquadra cuentan con la Ley 10/1994, de 11 de Julio, de la Policía de la Generalitat-Mossos d'Esquadra, que es el instrumento normativo que regula su régimen

[38] L.O. 3/1979, 18 de diciembre, Estatuto de Autonomía del País Vasco.
[39] Información disponible en: https://www.ertzaintza.euskadi.eus/lfr/web/ertzaintza/-/grupo-especializado-scdti (Fecha de consulta:16 de abril de 2022).

de funcionamiento, organización y funciones. Esta norma, en su sección III, del Capítulo I, a las Unidades de Policía Judicial, le atribuye las mismas competencias y obligaciones que las Fuerzas y Cuerpos de Seguridad del Estado.

En la Disposición Final Segunda de la L.O. 2/1986, se dispone que los Mossos d'Esquadra se regirán de acuerdo a su Estatuto de Autonomía y normas que lo desarrollen, siendo esta L.O. de carácter supletorio. Los Mossos d'Esquadra cuentan desde 2014 con la Unidad de Ciberseguridad (UCIBER).

La Policía Foral de Navarra, que contaba con competencias plenas en cuestión de Policía Judicial desde la Ley Foral 8/2007, de 23 de marzo, no había asumido dichas competencias. Es a raíz de la aprobación de la Ley Foral 23/2018, de 19 de noviembre, de las Policías de Navarra, que empieza a tener mayor trascendencia su área de Investigación Policial, donde encontramos su división de Policía Científica, que a día de hoy cuenta con el denominado Grupo de Delitos Informáticos, donde podemos ubicar el posible uso del agente encubierto informático[40].

1.1.4 POLICÍAS LOCALES

Las Policías Locales, de acuerdo con lo previsto en la L.O. 2/1986, pueden ser creadas en los municipios.

Las funciones de estos cuerpos policiales se detallan en el articulo 53 de dicha L.O., donde se especifica que, en materia de Policía Judicial, tienen atribuidas las competencias para instruir atestados por accidentes de circulación dentro del casco urbano o vías de su titularidad, así como participar como colaboradores de las Fuerzas y Cuerpos de Seguridad del Estado.

[40]Información disponible en la web del gobierno Navarro: https://www.navarra.es/home_es/Gobierno+de+Navarra/organigramas+departamentos/organigrama+departamento+presidencia+igualdad+funcion+publica+e+interior.htm?idunidadactual=10004117 (Fecha de consulta: 10 de mayo de 2.022).

Si bien es cierto que algunos municipios cuentan, excepcionalmente, con Unidades de Policía Judicial en su sentido estricto. Esta excepción es posible gracias al Convenio Marco de colaboración, cooperación y coordinación entre el Ministerio del Interior y la Federación Española de Municipios y Provincias en materia de seguridad ciudadana y seguridad vial, elaborada el 20 de febrero de 2007[41].

Los cuerpos policiales locales podrán adscribirse a Convenios de Colaboración con el Ministerio del Interior o con sus respectivas Comunidades Autónomas (siempre y cuando éstas tengan atribuida de forma expresa esta competencia), que les habilitarán para realizar funciones de policía judicial en lo relativo a recepción de denuncias, así como a la investigación de los hechos.

Dichas funciones sólo podrán ser de su competencia atendiendo a una serie específica de infracciones penales , relacionados con la actividad municipal o dentro del ámbito territorial del municipio, entre los que se destacaría los delitos contra la seguridad vial, algo acertado, ya que estos cuerpos policiales están especializados en esta competencia, así como cuentan con medios técnicos muy específicos (como serían los aparatos de detección y medición de alcohol o drogas en el organismo, así como servicios de retirada y depósitos de vehículos), que garantizan al ciudadano una seguridad, calidad y eficacia policial.

En cualquier caso, no quedan contemplados los delitos a través de la red, por lo que quedaría descartada su implicación en investigaciones que requieran del uso de la figura del agente encubierto informático, más allá de la cooperación con los cuerpos que sí tienen atribuidas esas competencias.

Creo necesario dotar a estos cuerpos, que tienen un conocimiento más cercano de los sucesos dentro de su territorio, de la posibilidad de formación y aplicación de la figura de agente encubierto informático dentro de sus competencias.

[41] Para más informaciónn, visitar: http://www.interior.gob.es/noticias/detalle/-/journal_content/56_INSTANCE_1YSSI3xiWuPH/10180/1135688/ (Fecha de consulta: 20 de abril de 2.022).

1.1.5 CENTRO NACIONAL DE INTELIGENCIA

El Centro Nacional de Inteligencia es, tal y como se define en su propia web, un servicio de inteligencia especializado que facilita al gobierno y su presidente información, análisis, estudios y propuestas con el fin de mantener la seguridad del Estado. Su responsabilidad es la de prevenir o evitar cualquier peligro, amenaza o agresión a la integridad territorial de España, los intereses nacionales, la estabilidad del Estado de derecho y sus instituciones[42].

El CNI se rige por el principio de sometimiento al ordenamiento jurídico y se encuentra regulada su actividad en la Ley 11/2002, de 6 de mayo, reguladora del CNI y la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Dentro del CNI encontramos el Centro Criptológico Nacional (CCN), creado en el año 2004, a través del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional. Es el organismo responsable de la seguridad de las tecnologías de la información y de protección de la información clasificada, compartiendo medios, procedimientos, normativa y recursos con el CNI.

Podríamos entender que, en el supuesto de seguridad del estado, el CNI podría llegar a contar con autorizaciones judiciales que legitimen vigilar a sospechosos de ciertos delitos muy concretos, como el terrorismo, si bien sus miembros no son agentes de la Policía Judicial.

A día de hoy, mientras me encuentro redactando este trabajo, nos encontramos con el "escándalo del Caso pegasus", en el que se ha visto involucrado en CNI en cuestiones de espionaje a diferentes políticos, entre otros, pertenecientes al gobierno independentista catalán o incluso el mismo presidente del gobierno[43].

[42] Página oficial del CNI: https://www.ccn-cert.cni.es/sobre-nosotros/centro-nacional-inteligencia.html (Fecha de consulta:14 de mayo de 2.022).

[43] https://www.lavanguardia.com/politica/20220504/8240943/escandalo-espionaje-extiende-tentaculos-presiona-sanchez.html (Fecha de consulta: 7 de junio de 2.022).

Esto se ha llevado a cabo a través del programa de espionaje ¨pegasus", que puede ser vendido o alquilado por una empresa israelí a organismos públicos (policía, ejercito o servicios de inteligencia), siendo un requisito indispensable que el uso del mismo esté destinado única y exclusivamente en investigaciones de casos de terrorismo o posibles delitos[44].

Éste software se instala de manera secreta en teléfonos móviles y permite un control pleno sobre el mismo, pudiendo activar cámaras, micrófonos, escuchar llamadas, leer conversaciones y obtener capturas de pantalla, así como rastrear la ubicación del mismo.

La intromisión en la vida del espiado es tan grande, que nos encontramos ante una investigación sobre si se contaba o no con las autorizaciones judiciales pertinentes para dichos rastreos, y si los cuerpos implicados han actuado en todo momento bajo el amparo de la legalidad[45].

Quizá con este caso se haya puesto en evidencia la falta en nuestro sistema de unas normas bien definidas para este tipo de actuaciones.

1.2. DIFERENCIAS CON EL AGENTE PROVOCADOR, EL CONFIDENTE Y EL ARREPENTIDO

Cuando conceptualizamos al agente encubierto informático, es importante diferenciarlo de otras figuras que podemos encontrar dentro de las diferentes investigaciones criminales. Las más destacables serían el agente provocador, el confidente y el arrepentido.

[44] https://cadenaser.com/2022/05/02/como-funciona-pegasus-asi-infecta-este-software-maligno-los-telefonos-de-politicos/ (Fecha de consulta: 15 de mayo de 2.022).
[45] https://www.cope.es/actualidad/espana/noticias/que-pegasus-software-con-que-supuestamente-fueron-espiados-los-independentistas-20220421_2038261 (Fecha de consulta: 15 de mayo de 2.022).

1.2.1 EL AGENTE PROVOCADOR

El agente provocador no se encuentra regulado en nuestro ordenamiento jurídico, si bien podemos llegar a definirlo a través de la jurisprudencia que se ha venido recogiendo sobre esta figura[46].

Podemos definir al agente provocador como aquel que induce a la comisión de un delito, provocando a un tercero para que tome la iniciativa de delinquir[47]. La finalidad de dicha figura es la de demostrar la implicación del provocado y obtener pruebas convincentes.

Según PERALS CALLEJA, "el denominado impropiamente agente encubierto se asemeja a la figura del agente provocador en que se trata de un funcionario policial que se acerca a una organización de delincuentes, escondiendo su condición de funcionario público, fingiendo intervenir en el delito y de esta manera provoca la consumación del mismo. Se distingue claramente de la figura recogida en el art 282 bis LECrim porque aquí no es necesaria una identidad ficticia ni previa autorización judicial"[48].

Por lo tanto, a consecuencia de esta inducción a la comisión de un delito, surge como consecuencia un delito provocado, definido en la STS 591/2018 como "aquel que llega a realizarse en virtud de la inducción engañosa de un agente que, deseando conocer la propensión al delito de una persona sospechosa y con la finalidad de constituir pruebas indubitables de un hecho criminal, convence al presunto delincuente para que lleve a cabo la conducta que de su torcida inclinación se espera simulando primero allanar y desembarazar el *inter criminis*[49] y obstruyéndolo finalmente, en el momento decisivo, con lo cual se consigue que por el provocador no sólo la casi segura detención del inducido sino la obtención de pruebas que se suponen directas e inequívocas".

---

[46] Véase STS 591/2018, de 26 de noviembre de 2018.
[47] Entre otras definiciones, pueden leerse la de
MUÑOZ SÄNCHEZ; J:, *El agente* provocador Monografías 36, Valencia 1995, p.43.
PERALS CALLEJA, J. "Técnicas de investigación del crimen organizado: el agente encubierto, confidente, regulación en España y validez de la prueba obtenida en el extranjero, problemas práctica de la heterogénea regulación de la materia", *Cuadernos digitales de formación*, 2010, p. 43.
[48] PERALS CALLEJA, J. "Técnicas de… *Op.Cit.*, p. 18.
[49] El *iter criminis* o camino del delito son las diferentes fases que atraviesa una persona desde que en su mente se produce la idea de cometer un delito hasta que efectivamente lo lleva a cabo.

En la regulación del agente encubierto informático, se define como límite de su actuación el uso de este comportamiento, ya que la intención de delinquir debe estar tomada por parte del delincuente, sin que la actuación del agente policial incite a la comisión de un delito.

Lo que se persigue con el agente encubierto informático, será siempre el descubrimiento del delito cometido, de acuerdo con el artículo 282 bis de la LECrim, 5) "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".

El artículo 9 de la Constitución, en su apartado 3, impide la arbitrariedad de los poderes públicos, por lo que se entiende que, al no limitar una actuación policial en la investigación de un delito, ésta será considerada ilícita, lo que implica la nulidad de las pruebas obtenidas a través del uso de la figura del agente provocador. "La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos"[50].

En este sentido es relativamente habitual la presentación de recursos por parte de la defensa que alegan que la actuación del agente policial como agente infiltrado ha traspasado su funciones actuando como agente provocador. Un ejemplo de ello sería la STS 21/2022, de 13 de enero de 2022, en la que la policía judicial portuguesa comunica a la policía judicial española, las sospechas sobre dos personas que, pertenecientes a una organización criminal, se disponían a trasportar grandes cantidades de cocaína a España a través del aeropuerto.

Dos agentes de la policía judicial española, concretamente del grupo de drogas de la Unidad Central Operativa de la Guardia Civil, acuden como personas relacionadas con la descarga de la droga en el aeropuerto a una reunión con los imputados.

[50] Dicho precepto así lo señala.

Posteriormente, la unidad policial a cargo de la investigación informa a la Fiscalía Especial Antidroga de la Audiencia Nacional, quien autoriza la actuación de dichos agentes como agentes encubiertos y es a partir de ese momento que dichos agentes mantienen comunicaciones con los imputados, recabando así pruebas de las tentativas delictivas de los mismos.

Los imputados, en el caso de autos, consideran que se ha producido una provocación al delito, presentado un recurso a este respecto, siendo éste desestimado por la autoridad judicial, motivando su resolución al entender que "la intervención policial, en funciones de agente encubierto, es posterior a la iniciación del delito, este es preexistente al tiempo de la intervención de los agentes que se limitan a levantar, a poner en claro, una situación antijurídica preexistente".

Se declara probado que los acusados estaban en posesión de la sustancia tóxica antes de la intervención policial como agentes encubiertos, no paralizando éstos la acción delictiva, sino procediendo a su detención una vez descubierto y asegurado el acto de tráfico, donde los agentes encubiertos actuaron debidamente autorizados, simulando su participación en la recepción de la misma".

En definitiva, el indicador principal para determinar que un agente no ha actuado como agente provocador, sería la confirmación de la actividad criminal previa a la actuación del mismo, lo que indicaría que no ha sido la inducción a delinquir el desencadenante del delito.

Por tanto, en la práctica, pueden darse situaciones ambiguas, en las que será una delgada línea la que separe la correcta actuación del agente encubierto informático de la actuación como agente provocador. La infiltración puede dar lugar a una cooperación material con el investigado, pudiendo implicar una participación en el hecho delictivo.

Es por ello que creo imprescindible que se respete la continua comunicación con las autoridades judiciales, estudiar las circunstancias concretas del mismo, y resolver en cada caso dónde situar el límite de la actuación policial, con el fin de no traspasar dicha línea.

La labor del agente encubierto informático ha de ir encaminada al descubrimiento de delitos ya cometidos, con el fin de poner término a la actividad delictiva, pero siempre utilizando técnicas que persigan descubrir los canales o redes a través de los cuales se vienen desarrollando los hechos ilícitos, respetando siempre que la trasgresión de las normas nazca libremente de la voluntad del autor[51].

Cabe aquí hacer un inciso en la normativa que regula al agente encubierto informático, ya que se contempla en ella una serie de actuaciones concretas que, entre otras, autoriza el envío de archivos que pueden ser considerados ilícitos por parte del agente policial judicial, de este tema se hablará con más detalle más adelante.

Cuando es el propio agente policial quien induce a la comisión de un delito, se entiende que, al ser el agente quien injerta el dolo de delinquir en un tercero, no existe culpabilidad del investigado, sino un delito provocado, por tanto no habría infracción penal, ya que al procederse a su detención antes o en el mismo instante en el que se lleva a cabo la comisión del delito, se estaría entrando en el terreno de lo que se define como un delito imposible.

Siendo estos actos realizados en fase pre-procesal, el atestado y prueba obtenidas carecerán de validez, dando lugar a la absolución de los implicados. Además, esta actuación atenta contra los principios de legalidad del proceso e interdicción de la arbitrariedad de los poderes públicos, al igual que contra la dignidad de la persona, así como al de un proceso con todas las garantías, principios recogidos en la Constitución Española[52].

En otros países como Estados Unidos, tal y como nos detallan BERGMAN Y BERMAN, se hace una diferenciación entre el delito provocado con o sin previa predisposición a delinquir del investigado. Esto es, a la hora de declarar la exención o

[51]ALCOLADO CHICO, M.T., "La evolución hacia la moderna funcionalidad del "agente encubierto": incidencia de las nuevas reglas de la ley de enjuiciamiento criminal" *Revista jurídica de Asturias* Madrid, 2016, nº39, pp.:7-32.
[52] Véanse los artículos 9.3, 24 y 25.

no, de la responsabilidad penal de quien comete un hecho ilícito, se valora la existencia o no del denominado *"entrampment"*[53].

Se conoce como *"entrampment"* a la interacción de los agentes policiales con el acusado, antes o durante la ejecución del hecho delictivo, cuando se utilizan técnicas como la coerción, amenazas o acoso, incluso halagos, para inducir a los investigados a la comisión del delito. Así, cuando existe una evidencia de esta trampa por parte de los agentes policiales, conllevará a una exención de responsabilidad penal del acusado.

Ahora bien, si queda probado que los agentes policiales simplemente proporcionaron oportunidades y facilidades para la comisión de un delito, existiendo una predisposición del investigado a cometer el mismo, se entiende que la actuación del agente provocador no legitima dicha conducta, resultando en una práctica totalmente aceptable.

1.2.2 EL CONFIDENTE

El confidente es una figura muy diferenciada del agente encubierto informático, siendo habitual su cooperación con el mismo[54]. Se trata de un persona que, perteneciendo a círculos delictivos o guardando cierta relación con la actividad delictiva, proporciona a los Cuerpos y Fuerzas de Seguridad información sobre los hechos criminales, quedando registrada esta información dentro del ámbito de las primeras diligencias policiales de carácter extraprocesal[55].

Las motivaciones que pueden llevar a un ciudadano a colaborar con las autoridades pueden ser tanto el civismo en estado puro, como por intereses personales, como podría ser una retribución económica (algo que no parece factible en la actualidad) o la agilización de trámites administrativos (como podrían ser los de residencia, reagrupación familiar o nacionalidad…)[56].

---

[53] VVAA, *The criminal law handbook: know your rights, survive…*, Ed. NOLO, Estados Unidos, 2011.
[54] REDONDO HERMIDA, A., "El agente encubierto en la Jurisprudencia española y en la doctrina del TEDH", *La Ley Penal*, España, enero 2008, p.96.
[55] DELGADO MARTÍN, J., *Criminalidad organizada*, J.M.Bosch Editor, Barcelona, 2001, p.131.
[56] Para profundizar en el tema, pueden leerse estudios como el realizado por BILLINGSLEY, R.; NEMITZ, T. y BEAN, P.; «Informers: policing, policy, practice», Ed. Willan, Oregón, 2001, pp. 86- 89.

Hay que valorar también uno de los principales riesgos que presenta esta figura, que sería la veracidad o no de la información facilitada, ya que existe la posibilidad de que el confidente actúe como tal motivado por la venganza o rivalidad con los propios delincuentes, pudiendo ser la información proporcionada falsa o incluso incompleta por miedo a inculparse.

Por lo tanto, podríamos comparar la información que proporciona el confidente, con la información a la que accede un agente policial a través de una red abierta, lo que se conoce como ciberpatrullaje, algo en lo que se profundizará más adelante en este trabajo.

Servirá esta información para comenzar con una investigación preprocesal que recabe suficientes indicios que, una vez contrastados, serán suficientes para solicitar una autorización judicial. Dicha autorización conllevará a la apertura de diligencias procesales, siendo éstas debidamente fundamentadas, para así poder seguir con la investigación.

La identidad de la figura del confidente debe estar absolutamente protegida, siendo las autoridades las únicas conocedoras de la misma, ya que podría dar lugar a represalias de los supuestos delincuentes contra su persona y además, puede ser utilizada como fuente de información en un futuro[57]. Por tanto, se justifica acertadamente esta protección a la identidad del confidente, así como a las técnicas policiales pre-procesales, con el fin de garantizar la eficacia de las mismas.

El contenido de la investigación pre-procesal, así como las colaboraciones con los agentes policiales, son acciones necesarias para fundamentar las sospechas de la comisión de los hechos delictivos, y por tanto, no repercuten legalmente en el futuro material probatorio de los mismos.

[57] HARFIELD, C.; "Police informers and professional ethics", *Criminal Justice Ethics*, vol.31, n.º2, https://www.tandfonline.com/doi/abs/10.1080/0731129X.2012.696960 2012, pp.73-95.

Una vez concluida la investigación pre-procesal, que en ningún caso traspasará al plano de una limitación o quebrantamiento de los derechos fundamentales del investigado, es cuando el control y autorización judicial resultan imprescindibles, para así poder asegurar que se cumplen los principios de equilibrio y defensa recogidos entre los derechos del detenido.

Un ejemplo de ello lo encontramos en la STS 312/2021, de 13 de abril, el la que la defensa presenta un recurso, solicitando los detalles de la investigación pre-procesal, en la que existe una comunicación por parte del FBI a la Unidad de la UCO de la Guardia Civil, persiguiendo un delito de blanqueo de capitales, que desencadena en una detención por tráfico de drogas a dos sujetos que no eran, en primera instancia, el objeto de dicha investigación.

Se justifica dicho recurso por entender que no se ha respetado el derecho de todo detenido a que se le faciliten los documentos relacionados con el atestado de su detención, derecho amparado por la Directiva 2012/13 EU del Parlamento Europeo, específicamente en su artículo 7.

Entiende el Tribunal Supremo en su fallo, que no existe un derecho a que al encausado se le desvele el contenido de las informaciones dada por el confidente, o por colaboraciones policiales internacionales, así como las técnicas de investigación policial, mientras no repercutan legalmente sobre el material probatorio que fundamenta la acusación.

Tal y como detalla PERALS CALLEJA, la figura del confidente carece de regulación, aún estando presente en numerosas actuaciones policiales [58]. A este respecto se pronuncia ya en 2004 la comisión de investigación del 11-M, haciendo constar que es imprescindible su regulación, y siendo a día de hoy un tema todavía señalado[59].

El confidente puede acudir a los agentes policiales por iniciativa propia, así como ser instado por los mismos a facilitar una serie de datos o realizar una investigación. La

[58] PERALS CALLEJA, J. "Técnicas de investigación…"*Op. Cit*., p. 28.
[59] https://www.elindependiente.com/politica/2020/03/02/la-figura-del-confidente-sigue-sin-regularse-casi-15-anos-despues-del-dictamen-del-11-m/ (Fecha de consulta: 12 de abril de 2022).

información proporcionada por el mismo es considerada como indicio a la hora de iniciar una investigación, pero no será suficiente como prueba para fundamentar una resolución judicial o condena[60]. El confidente podrá serlo de manera puntual, al hacer llegar ocasionalmente a las autoridades información acerca de una actividad ilícita, así como habitual, manteniendo un flujo de información de manera más o menos frecuente con las mismas. Distinto del confidente sería el denunciante anónimo, que facilita los datos de forma altruista a las autoridades.

En determinados casos, puede darse una infiltración del confidente, bien por propia iniciativa, bien por causas sobrevenidas al ser una persona que ya tiene un contacto previo con los delincuentes investigados.

Aquí habría que recalcar que, aún cuando la figura del colaborador queda avalada por diferentes resoluciones judiciales, reconociéndola como una fuente lícita de información, no estando la misma reconocida en nuestra legislación, y al no tratarse de un agente policial, cualquier acto ilícito por parte de la misma realizado con el fin de obtener información sobre la actividad delictiva, no estaría exento de responsabilidad criminal[61].

1.2.3 EL ARREPENTIDO

El arrepentido es un individuo que, perteneciendo a un grupo criminal, decide confesar sus propios crímenes, así como colaborar con la justicia mediante el suministro de información. Los datos proporcionados por parte de esta figura serán relativos a organizaciones delictivas, con el fin de esclarecer delitos e incluso evitar otros futuros, tal y como detalla DIAZ MAROTO Y VILLAREJO[62].

[60] GÓMEZ DE LIAÑO FONSECA-HERRERO, M. *Criminalidad organizada… Op. Cit...*, p.150.

[61]MARCHAL GONZÁLEZ, A.N., "Precisión terminológica en torno a la figura del confidente en el proceso penal", *Diario La Ley*, nº9083, España 2017, pp.2-7.

[62] DÍAZ MAROTO Y VILLAREJO, J., "Algunos aspectos jurídico penales y procesales de la figura del arrepentido", *Diario La Ley*, nº 5, España 1996, p.1463.

La figura del arrepentido está prevista en nuestro ordenamiento jurídico en el delito de tráfico de droga (art 376 CP) y en el de terrorismo (art 579). Será requisito indispensable la participación de esta persona en los hechos enjuiciados.

Se prevé para este sujeto, en el artículo 376 del Código Penal, unos beneficios punitivos, en forma de atenuantes de confesión del delito (art. 21.4 CP) y reparación del daño ocasionado o disminución de sus efectos (art. 21.5), para aquel que colabora con las autoridades con el fin de impedir la producción de delitos, obtener pruebas para la identificación de otros integrantes de bandas organizadas, así como evitar las actuaciones de las mismas.

Aunque el arrepentido no se trata de un informador anónimo, tal y como sucede con el confidente, se beneficiará igualmente de la protección de su integridad personal por parte de las autoridades. Dicha protección se encuentra regulada por la resolución del Consejo de 23 de Noviembre de 1995, de protección de testigos en el marco de la lucha contra la delincuencia organizada internacional, y por la Resolución del Consejo de 20 de diciembre de 1996, relativo a las personas que colaboran en la lucha contra el crimen organizado.

La declaración como testigo por parte del arrepentido, será constitutiva de una prueba de cargo en el proceso judicial, siendo exigida su participación en los hechos enjuiciados y su imputación. Esta figura se contempla como una infiltración sobrevenida, controlada por el poder público[63].

Como apunta GASCÓN INCHAUSTI, se plantean dificultades en la actuación del arrepentido, ya que sus declaraciones, al tratarse de un coimputado, pueden generar dudas con respecto a su veracidad, así como en lo relativo a concretar su responsabilidad penal[64].

Esta figura, además de no contar con la condición de agente policial, se diferencia del agente encubierto informático en que no es necesaria la ocultación de su identidad, así

[63]GÓMEZ DE LIAÑO FONSECA-HERRERO, M. "Criminalidad organizada y… Op. Cit.", p.150.
[64] GASCÓN INCHAUSTI, F. "Infiltración policial y agente encubierto", Comares, Granada, 2001, p.25.

como lo será el requisito de imputación exigido en el proceso, diferenciándola así también del confidente.

Una vez definidas las diferentes figuras, considero que es necesaria una regulación de las mismas, especialmente la del agente provocador, siendo ésta la que más problemática en referencia a la multitud de recursos que se realizan contra investigaciones en las que el agente encubierto ha tenido un papel fundamental.

2. ANTECEDENTES: EL AGENTE ENCUBIERTO FÍSICO

La figura del agente encubierto informático es la evolución, necesaria, de una figura anterior, el conocido como agente encubierto, que opera en terrenos físicos y se utiliza como infiltración en actuaciones contra la delincuencia organizada para así poder investigar conductas delictivas que serían difícilmente perseguibles de otro modo[65].

Tal como explica LÓPEZ YAGÜES, el agente encubierto nace de la necesidad por parte de los Estados y la Sociedad Internacional en su conjunto, de salvar las dificultades en materia de obtención de elementos probatorios sobre la autoría o la existencia de delitos desarrollados por el crimen organizado, así como de evitar los delitos futuros de estas organizaciones, que se caracterizan por generar daños incuantificables en cuanto a bienes e intereses individuales, colectivos y sistemas económicos y político-sociales[66].

Los mecanismos de autoprotección del crimen organizado son de especial dificultad, debido a su clandestinidad, silencio y opacidad entre otras características[67], por lo que a a mi juicio, venían haciendo indispensable la regulación del agente encubierto y su aplicación en ciertas investigaciones.

[65] Así lo prevé el art.282 LEcrim, en los puntos 1 y 4, si bien sería deseable que se ampliase a la investigación de otros delitos.
[66] LÓPEZ YAGÜES, V., "El agente encubierto", en *Derecho procesal penal* (Coord. FUENTES SORIANO, O.), Tirant lo Blanch, Valencia, 2020, pp.192-193.
[67] EXPÓSITO LÓPEZ, L., "El agente encubierto", *Revista de derecho, UNED,* https://doi.org/10.5944/rduned *nº*17, 2015, p.255.

Por lo tanto, el concepto de legal de agente encubierto, establecido en el art. 282 bis LECrim, dentro del Título III: de la Policía Judicial, recoge el término agente en referencia a agente policial, así como encubierto, con respecto a la ocultación de su identidad, condición e intenciones como policía[68].

En la sentencia STS 1140/2010, de 29 de diciembre de 2010, se define al agente encubierto de la siguiente manera: "El término undercover o agente encubierto, se utiliza para designar a los funcionarios de policía que actúan en la clandestinidad, con identidad supuesta y con la finalidad de reprimir o prevenir el delito. Agente encubierto, en nuestro ordenamiento, será el policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la Ley y bajo el control del Juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación o estos sean insuficientes, para su descubrimiento y permite recabar información sobre su estructura y modus operandi, así como obtener pruebas sobre la ejecución de hechos delictivos, debiéndose aclarar que es preciso diferenciar esta figura del funcionario policial que de forma esporádica y aislada y ante un acto delictivo concreto oculta su condición policial para descubrir un delito ya cometido"[69].

La figura del agente encubierto físico se encuentra regulada en el art. 282 bis LECrim, a través de una reforma referente a la actividad investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves, efectuada por la Ley 5/1999, de 13 de Enero, y tras su inclusión en nuestro ordenamiento jurídico, se establecen a través del art. 282 bis unos requisitos y límites para su actuación[70].

El Ministerio Fiscal o bien el Juez de Instrucción competente será quien, mediante resolución fundada y teniendo en cuenta la necesidad de dicha figura para los fines de la investigación, autorizará a funcionarios de la Policía Judicial a actuar bajo identidad supuesta, así como a la adquisición y transporte de objetos, efectos e instrumentos del delito y a diferir la incautación de estos.

[68] SANCHEZ TOMÁS, JM., *Derecho de las drogas y drogodependencias*, FAD, Madrid, 2002, p.214.
[69] STS 1140/2010, de 29 de diciembre, de 2010, FJ 6º.
[70] GIMENO SENDRA, J.V., *Derecho procesal penal*, Editorial Civitas, Navarra, 2012, p.14.

Como matiza DELGADO MARTÍN, los límites temporales de la medida serán establecidos por el órgano judicial que autorice la misma, valorando la necesidad, proporcionalidad y riesgos presentes en la infiltración[71]. Si bien no puede ser concedida por plazos superiores a seis meses, prorrogables por períodos de igual duración, nada impide que se acuerde por un plazo inferior si así es valorado atendiendo al principio de proporcionalidad. Cabe deducir que la infiltración durará el tiempo que se considere necesario a los fines de la investigación.

Estas medidas son especialmente importantes, ya que nacen de la necesidad de legitimar la figura del agente encubierto, ya que puede afectar a derechos fundamentales, tales como el derecho a la intimidad, la inviolabilidad del domicilio o el secreto de las comunicaciones, que podrían verse comprometidos. Como apunta GIMENO SENDRA, pese a tratarse la figura del agente encubierto de una medida altamente restrictiva de derechos fundamentales, la introduce el legislador con el artículo 282 bis dentro de los preceptos reguladores de la policía judicial, posiblemente para resaltar la importancia del papel de estos agentes policiales en el desarrollo de la investigación[72].

Debe respetarse la voluntariedad del funcionario de la Policía Judicial a actuar como agente encubierto, así como a mantener dicha identidad cuando testifiquen en el proceso judicial el cual se derive de dicha investigación, siempre que así se acuerde mediante resolución judicial motivada, según lo previsto en la Ley Orgánica 19/1994, de 23 de diciembre. Este es un aspecto importante debido a la peligrosidad y riesgos a los que el agente policial se enfrenta con esta práctica.

El agente encubierto deberá solicitar al órgano judicial competente las autorizaciones necesarias que se establezcan de acuerdo a la Ley y la Constitución cuando se puedan ver comprometidos los derechos fundamentales debido a las actuaciones de investigación. Estas autorizaciones deben estar motivadas y ser precisas, así como obedecer a un fin legítimo y ser proporcionales. Además, deberá poner en conocimiento de quien autorizó la investigación, de la información que se vaya resolviendo a raíz de

[71] DELGADO MARTÍN, J., *La criminalidad organizada. Comentarios a la Ley 5/1999 de 23 de febrero,* Bosch, Barcelona, 2001, p.16.
[72] GIMENO SENDRA, J.V., *Derecho procesal… Op. Cit.,* pp.14-15.

ella a la mayor brevedad posible, estando en manos del órgano judicial competente la determinación del modo en que será llevado a cabo este trámite[73].

El ámbito de actuación del agente encubierto físico será el de las investigaciones relacionadas con actividades propias de la delincuencia organizada, entendiéndose como tal a la asociación de tres o más personas, para realizar conductas delictivas de manera permanente o reiterada, que se encuentran enumeradas en el punto cuatro del mencionado artículo y que serían los delitos previstos en el Código Penal relativos al secuestro de personas, prostitución, contra el patrimonio y el orden socioeconómicos, contra los derechos de los trabajadores, el tráfico de especies de flora o fauna amenazada, de tráfico de material nuclear y radiactivo, contra la salud pública, la falsificación de moneda, el tráfico y depósito de armas, municiones y explosivos, terrorismo y contra el Patrimonio Histórico[74].

La ley detalla la exención de responsabilidad criminal en su actuación, siempre que ésta sea una consecuencia necesaria para el desarrollo de la investigación, se guarde la debida proporcionalidad con el desarrollo de la misma y no constituyendo una provocación al delito.

Con respecto a este punto, no siendo lo suficientemente específico y dando pie a interpretaciones personales, la jurisprudencia se ha tenido que pronunciar ante numerosas alegaciones presentadas por la defensa, en recursos en los que se argumenta que el agente encubierto actúa más bien como un agente provocador, tal y como se ha detallado anteriormente[75].

[73] Así se refleja en la STS 395/2014, 13 de mayo de 2014, en la cual se consideró irregular la actuación de un agente encubierto, por incumplir el deber de información y de comunicar el resultado íntegro de la investigación, al no comparecer en el juicio oral.
[74] SANCHEZ TOMÁS, JM., *Derecho… Op. Cit.*, p.214.
[75] SSTS 406/2012, de 7 de mayo de 2012; 204/2013, 14 de marzo de 2013; 575/2013, 28 de junio de 2013.

3. NATURALEZA JURÍDICA

La aparición de internet crea escenarios en los que han ido apareciendo nuevos hechos delictivos no contemplados en nuestro Código Penal. Esta situación es también un problema internacional, crea una serie de debates a nivel mundial y una necesidad por parte de los distintos legisladores de adaptar sus leyes. Al mismo tiempo, pone sobre la mesa la conveniente creación de diferentes unidades específicas que deberán colaborar y coordinarse entre ellas con el fin de minimizar los efectos tan negativos de esta relativamente nueva delincuencia.

En marzo del año 2011 comienzó a debatirse en el Senado español la urgencia de regulación de la figura del agente encubierto informático, ante la necesidad, entre otras, de dotar de una herramienta a los agentes implicados en la lucha contra la pornografía infantil, siendo España en ese momento el segundo país de mayor consumo [76]. Finalmente, en 2015 se materializa esta petición, instando por lo tanto al Gobierno a presentar ante las Cortes Generales un proyecto ley de modificación de la LECrim y del Código Penal, ya que en nuestra legislación no existía una previsión legal más allá de delitos por tráfico de drogas o terrorismo.

Cabe destacar que la mayoría de los delitos informáticos no se encuadran en las exigencias detalladas en la reforma de la LECrim del año 1.999, y mucho menos en lo relativo a la delincuencia organizada o grupos criminales, ya que más bien son personas individuales que realizan estos actos desde el anonimato que les brinda la Red[77]. Esto deja a la figura del agente encubierto fuera de investigaciones tales como los daños informáticos o las estafas informáticas.

Ante la falta de una normativa sobre ciertos supuestos, éstos venían siendo atendidos en base a la jurisprudencia, siendo los jueces quienes iban creando una línea de actuación

[76] Diferentes medios de comunicación se hacían eco de esta problemática, como por ejemplo el diario levante: https://www.levante-emv.com/espana/2011/03/23/policias-encubiertos-pedofilia-internet-13075695.html (Fecha de consulta: 13 de enero de 2022)

[77] En el portal estadístico de criminalidad, podemos comprobar las infracciones penales relativas a la cibercriminalidad, viendo un claro aumento en los últimos años, así como por grupos penales. En los datos recogidos del año 2020, vemos el fraude informático, amenazas y coacciones o la falsificación informática como los grupos penales con mayor incidencia. Para acceder a estos datos, puede remitirse a https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/portal/datos.html?type=pcaxis&path=/Datos5/&file=pcaxis (Fecha de consulta: 14 de marzo de 2022).

sobre la materia no recogida por la Ley. Así, con el fin de fortalecer las garantías procesales y regular las medidas de investigación tecnológica, se crea la figura del agente encubierto informático, con un marco de actuación más amplio que el de su predecesor, el agente encubierto físico.

Esta figura aparece en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECrim, con la introducción de los apartados 6 y 7 del art. 282 bis, donde figuran las previsiones necesarias para la integración de las nuevas técnicas y formas de infiltración en nuestro ordenamiento[78].

Si buscamos referencias a las TIC en la Constitución Española, es en la sinopsis 1 incluida en la web de la constitución, relativa al artículo 18.3, que garantiza "el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial". En ella se hace un inciso al carácter abierto de este enunciado, del cual cabe entender que se incluyen en este artículo las comunicaciones tales como el correo electrónico, chats o cualquier otro en el que esté involucrado un elemento ajeno a los sujetos que intervienen en el proceso de comunicación. La protección de las comunicaciones supone que éstas solo podrán ser intervenidas mediante resolución judicial y con las garantías previstas.

También encontramos en el artículo 18.4 una protección en forma de ley[79], al uso de la informática que garantice el honor e intimidad de los ciudadanos, ejerciendo plenamente sus derechos. Cabe señalar, tal y como se extrae de la STC 114/1984, que cuando uno de los intervinientes sea quien levante el secreto, no estaría violando este artículo, sino, en todo caso, vulnerando el derecho a la intimidad[80].

Es por lo tanto, con la regulación del agente encubierto del art. 282bis de la LECrim, donde encontramos una solución a las carencias que presentaban las técnicas empleadas

[78] "El legislador, motivado por las novedades tecnológicas y en su afán por actualizar las medidas de investigación de determinadas modalidades delictivas, se inclina por reforzar la figura del agente encubierto", VALIÑO CES, A., "Una lectura crítica en relación al agente encubierto informático tras la Ley Orgánica 13/2015", Diario La Ley, núm. 8731, 2016, p.3.
[79] Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
[80] STS 114/1984, 29 de noviembre de 1984.

en determinadas investigaciones relativas a conductas criminales, como serían los registros domiciliarios o intervenciones de comunicaciones, con el fin de completar la acción investigadora con respecto a la circulación y entrega vigilada de sustancias prohibidas, además de las drogas.

Manteniendo los requisitos y exigencias propios del agente encubierto físico, como serían entre otras la de necesidad de autorización judicial y la información continua por parte del agente al juez de instrucción, es con la introducción de los apartados seis y siete del citado artículo con los que encontramos regulada la figura en el ámbito virtual.

En el apartado 6 se especifica en primer lugar: "El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a."

Por lo tanto, se prevé su uso en investigaciones de delitos llevados a cabo por la delincuencia organizada dispuestos en el apartado 4, y en el artículo 588 ter a., que nos refiere al art. 579.1 LECrim, como serían los delitos de terrorismo, delitos cometidos en el seno de una organización criminal o delitos dolosos castigados con penas con un límite máximo de, al menos, tres años de prisión; o cualquier otro delito cometido a través de medios informáticos.

Es así como se soluciona el vacío legal existente a la hora de introducir la figura del agente encubierto en investigaciones de delitos cometidos a través de las redes, abriendo un abanico de posibilidades para su utilización, ya que como detalla en su estudio ZARAGOZA TEJADA, ante la falta de jurisprudencia que aclare si la figura del agente encubierto informático pueda o deba ser usado de manera única y exclusiva en el ámbito de la delincuencia organizada[81].

El apartado 6 del art. 282bis permitiría al juez de instrucción autorizar dicha figura en investigaciones en las que no exista esa nota de cooperación u organización, siempre

[81] ZARAGOZA TEJADA, J.I., "El agente…, Op. Cit. pp.199-203.

atendiendo a los criterios de proporcionalidad e idoneidad para no caer así en una dinámica de persecución de delitos poco lesivos o relevantes socialmente.

El apartado 6 continúa: "El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos."

Esta competencia está motivada, como detalla LAFONT NICUESTA entre otras causas, en la lucha contra delitos de distribución pornográfica infantil, ya que la emigración de las redes de pederastas a comunidades cerradas, creaba una necesidad de facilitar su investigación así como de considerar a los clubs cerrados de pederastas como organizaciones criminales[82].

Es en este punto donde se crea un debate social, debido a que, tal y como lo recoge LÓPEZ GARCÍA en su artículo, podría optarse por intercambiar por parte del agente archivos pornográficos en los que se haga uso de actores mayores de edad que se hiciesen pasar por menores [83].

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

Éstas grabaciones realizadas, al no contar con una regulación específica, se harán por lo dispuesto en el Capítulo VI "Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos"[84] .

[82] LAFONT NICUESA, L., "El agente encubierto en el proyecto de reforma de la Ley de Enjuiciamiento Criminal", Diario La Ley, núm. 8580, Julio 2015
[83] LÓPEZ GARCÍA, E., "Agente encubierto y agente provocador, ¿dos figuras incompatibles?" *Diario La Ley*, 2003. Nº4, p.1504-1506.
[84] art.588 quater a) a e) LeCrim.

Amparadas por el art. 282bis 3 LECrim, estas competencias serán previa autorización judicial habilitante, que deberá de basarse en la proporcionalidad de la medida, al ser ésta limitativa de los derechos fundamentales, argumentándose la idoneidad de ésta, su necesidad y el debido equilibrio entre el sacrificio del derecho fundamental limitado y la ventaja que se obtendrá del mismo en función de las circunstancias que rodeen a la investigación en curso.

Por lo tanto, se extrae de la lectura de estos puntos, que como características más específicas y a diferencia del agente encubierto físico, una vez decidida la utilización del agente encubierto informático, ésta deberá ser autorizada única y exclusivamente por el Juez de Instrucción y no así por el Ministerio Fiscal, para así "garantizar el pleno respeto del derecho a la intimidad y al secreto de las comunicaciones de las personas afectadas", tal y como se recoge en la Exposición de Motivos de la reforma.

Para navegar en los foros, chats y páginas web, en canales cerrados donde es necesario una identidad verificada, el agente contará con una identidad distinta a la real o un nombre conocido como *"Nickname"*, así como una identidad ficticia, que será otorgada por el Ministerio del Interior. Al no especificarse una limitación temporal a la autorización del agente encubierto informático, se entiende que se mantendrá la norma reguladora al agente encubierto físico, por plazo de máximo seis meses de duración, prorrogables[85]. Habrá que diferenciar esta identidad ficticia de la utilizada en canales abiertos de la red, que es totalmente lícita para la obtención de cualquier prueba, sin necesidad de autorización judicial.

Creo por lo tanto, que la creación de una identidad falsa para el agente encubierto informático será muy sencilla, existiendo una serie de ventajas para el Estado, puesto que a diferencia del agente encubierto tradicional (que requerirá de una diferente documentación, así como la necesidad de dotar de una vivienda y una vida paralela), serán necesarios simplemente una serie de datos personales básicos, suponiendo un coste económico mucho inferior.

[85] ZARAGOZA TEJADA, J.I., "El agente… *Op. Cit.*, p.204.

Por otro lado, el agente de la policía Judicial, en su valoración personal a la hora de actuar como agente encubierto informático, podrá ver como positivo que ni su imagen será pública, ni será necesario un contacto físico con los investigados. Aún así, tendrá que valorar las posibles consecuencias a nivel psicológico, al tener que mantener conversaciones con cierto tipo de delincuentes, como podría ser el caso de los pedófilos, ya que al hacerse pasar por uno de ellos, también tendrá que visionar contenido explícito

EPÍGRAFE 2. TIPOS DE ACTUACIÓN Y RESPONSABILIDAD DERIVADA DE LA MISMA.

Una vez realizada la regulación del agente encubierto informático, complementándose con otras medidas, como el registro domiciliario, las medidas reguladas en la LECrim en sus artículos 588, sobre la interceptación de las comunicaciones, así como toda la doctrina de la que disponemos, podemos definir las diferentes actuaciones por parte del agente encubierto informático, así como definir los límites de su actuación y responsabilidades.

1. INTERVENCIONES

Las técnicas de investigación criminal se han venido modificando debido al desarrollo tecnológico que experimentamos continuamente.

La permanente conexión a internet en la que vivimos, accediendo continuamente a nuestras redes sociales, correo electrónico y realizando búsquedas en la web, hace que datos muy precisos de nuestra personalidad sean accesibles a terceros, poniendo nuestra

intimidad y privacidad en peligro. Pero a su vez, se amplían el abanico de métodos para la investigación de hechos ilícitos, como apunta ZARAGOZA TEJADA[86].

La Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, es la respuesta del legislador a esta nueva realidad[87].

Es con esta modificación con la que se introducen nuevos mecanismos de investigación tecnológicos, como el acceso remoto a equipos informáticos (artículo 588 septies de la LECrim), el registro de dispositivos de almacenamiento de datos (artículo 588 sexies de la LECrim) o el agente encubierto informático (artículo 282bis de la LECrim, apartados 6 y 7).

En el preámbulo de la L.O. 13/2015, se indica que resulta preciso afrontar cuestiones como el "fortalecimiento de los derechos procesales de conformidad con las exigencias del Derecho de la Unión Europea y la regulación de las medidas de investigación tecnológica en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales garantizados por la Constitución".

Con los nuevos medios tecnológicos de investigación, además de los delitos relacionados con los nuevas tecnologías (como serían el phising, distribución de pornografía, etc.), otros delitos tradicionales pueden ser esclarecidos mucho más fácilmente, al contar con herramientas como la geolocalización de un Smartphone o la determinación de una dirección IP. Sin embargo, estos medios de investigación requieren de una necesidad de equilibrio entre la capacidad del Estado para perseguir estas actividades delictivas y la garantía constitucional de los ciudadanos frente a terceros.

Cuando se interviene un Smartphone, tablet u ordenador, en él pueden estar almacenados datos y archivos de diferente naturaleza (profesional, personal, de ocio,

[86] ZARAGOZA TEJADA, J., "Investigación tecnológica y derechos fundamentales, comentarios a las modificaciones introducidas por la ley 13/2015. El agente encubierto online" Editorial Aranzadi, 2017, pp.197-200.
[87] Enlace https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725

etc.). Accediendo a éstos dispositivos, podemos llegar a ciertos datos susceptibles de protección constitucional, como el derecho a la intimidad (recogido en el artículo 18.1 CE), el secreto de comunicaciones (recogido en el artículo 18.3 CE) y el de protección de datos (18.4 CE).

Por ejemplo, al leer o enviar un email, éste queda almacenado en un servidor al que se accede a través de nuestro dispositivo. Si mantenemos una conversación a través de *apps* de mensajería instantánea, éstas conversaciones y los documentos enviados a través de las mismas quedan almacenadas en ella. Igualmente, pueden estar almacenados, mensajes no enviados e incluso mensajes no leídos por el destinatario.
Podríamos decir que al igual que se entienden estos datos protegidos por el secreto de comunicaciones, al encontrarse almacenados una vez concluida esa comunicación, los mismos quedan protegidos por el derecho a la intimidad.

Éstos derechos requieren de una resolución judicial expresa, aún existiendo una autorización previa de registro e intervención de los dispositivos electrónicos de manera física. El derecho a la intimidad tiene una excepción por la que la policía, en caso de urgencia, puede llevar a cabo una intromisión de la misma. La Policía Judicial o el Ministerio Fiscal podrán realizar un registro de dispositivos y equipos telemáticos en casos de urgencia, informando inmediatamente al juez, con un plazo máximo de veinticuatro horas desde que se ha realizado esta actuación. El juez deberá revocar o confirmar tal actuación en un plazo de setenta y dos horas y, por tanto, cabe la posibilidad de que dicho material probatorio sea desestimado[88].

A día de hoy, se pone sobre la mesa el debate de un derecho que no contempla nuestra constitución, que sería el llamado derecho al entorno o intimidad virtual. En él se englobarían el derecho a la intimidad, el secreto de comunicaciones y el derecho a la protección de datos personales en su conjunto. Se entiende que cuando se obtienen los datos de un dispositivo por separado, los mismos pueden ser de carácter personal, íntimo o técnico, pero una vez se analizan en su conjunto, pueden describir aspectos

[88] ZARAGOZA TEJADA, J., "Investigación… *Op. Cit.*, p.197.

relevantes sobre la personalidad de su titular, que podrían servir para la elaboración concreta de un perfil[89].

Cabe aquí destacar la STS 204/2016, de 10 de marzo, donde se habla de este derecho: "el Legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual". Se hace mención en la citada sentencia, además, a una sentencia anterior, la STS 342/2013, de 17 de abril, que indica "…existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos…"

Como indica ARRABAL PLATERO, para proteger la información que a través de las tecnologías genera el usuario, se ha creado por la jurisprudencia esta garantía constitucional que es el derecho fundamental al propio entorno virtual.

Teniendo en cuenta todos estos supuestos, es con la regulación de la figura del agente encubierto informático, donde se amplían las conductas por las cuales se puede solicitar al Juzgado correspondiente el uso de la misma y se abre todo un abanico de posibilidades, tanto al autorizarse su uso dentro del ámbito de internet, como en los delitos a los que se puede aplicar, no siendo estrictamente necesaria la pertenencia a organizaciones criminales.

También se regulan diferentes niveles de infiltración policial. Tal y como detalla LAFONT NICUESTA[90], los marcos de actuación del agente encubierto informático

[89]ARRABAL PLATERO, P., «El derecho fundamental al propio entorno virtual y su incidencia en el proceso», en *Era Digital, Sociedad y Derecho* (Dir. FUENTES SORIANO; Coords. ARRABAL PLATERO, DOIG DÍAZ, ORTEGA GIMÉNEZ, TURÉGANO MANSILLA), Tirant Lo Blanch, Valencia, 2020, pp. 431-441.
[90] LAFONT NICUESTA, L., "El agente encubierto… Op. Cit. p.2.

serian dos: la actuación en canales abiertos o ciberpatrullaje[91] y la actuación en canales cerrados[92].

1.1. ACTUACIÓN EN CANALES ABIERTOS O CIBERPATRULLAJE

Como primer nivel de infiltración policial, nos encontramos con los rastreos policiales en espacio de libre acceso en la red.

Las Fuerzas y Cuerpos de Seguridad del Estado, realizan labores de investigación en la red de manera habitual[93]. Estas labores se realizan en foros abiertos de internet, en determinados ámbitos de redes sociales o en redes P2P, y se realizan tanto de forma directa, como por medio de procedimientos mecanizados. Dichas técnicas policiales se realizan atendiendo a las funciones de prevención del delito y son perfectamente válidas[94], no siendo exigibles unos requisitos especiales, como la autorización judicial previa[95].

Un ejemplo de ello sería la "Operación Araña", en la que agentes de la Guardia Civil llegaron a detener a setenta y siete personas, resultando más de cuarenta condenadas a penas de hasta dos años, por enaltecimiento del terrorismo en las redes sociales[96]. Estas detenciones fueron el resultado de serie de investigaciones realizadas por agentes expertos a través de canales abiertos de internet, apoyándose en herramientas de monitorización para búsqueda y análisis de información, así como por la colaboración

[91] Investigaciones realizadas por agentes policiales en el espacio público de la red, donde lo expuesto es accesible a cualquier usuario, sin necesidad de identificación. Es el primer paso a la hora de detectar posibles actos delictivos, con sospechosos no identificados.
[92] Investigaciones realizadas en espacios de la red donde es necesario identificarse para seguir entablando una comunicación el resto de usuarios.
[93] ZARAGOZA TEJADA, J.I., "*El agente encubierto online*", en Investigación tecnológica y derechos fundamentales (Coord. ZARAGOZA TEJADA), Editorial Aranzadi, Navarra 2.017, p.201
[94] Estas funciones de prevención del delito se establecen en el artículo 11 de la Ley de Fuerzas y Cuerpos de Seguridad, así como a la policía Judicial según lo establecido en el artículo 282 de la Lecrim, que indica que será su obligación averiguar los delitos públicos, practicar las diligencias necesarias para comprobarlos y descubrir a los delincuentes. Así también recoger los efectos, instrumentos o pruebas del delito para poner éstos a disposición de la autoridad judicial.
[95] Se regula la necesidad de autorización judicial previa, por lo que se actuaría como agente encubierto informático, únicamente en las investigaciones desarrolladas en canales cerrados de comunicación, lo que excluiría a los canales abiertos a esa necesidad dela misma.
[96] https://www.lainformacion.com/espana/diecinueve-detenidos-y-dos-imputados-por-apologia-del-terrorismo-en-redes-sociales_eclxboeh6tez2tphypwpa6/ (Visitado el 8 de junio de 2022).

ciudadana a través del portal "Colabora" y las redes sociales oficiales de la Guardia Civil. Al detectarse un gran número de perfiles en redes sociales desde los cuales se difundía contenido apologético de grupos terroristas, así como humillaciones a sus víctimas, los agentes policiales investigaban en estos canales abiertos si los autores de los mismos habían hecho otros con los que consolidar una denuncia.

En relación a esta operación se pronuncia el Instituto Armado, que con respecto a los comentarios difundidos en redes sociales por los que se motivó la investigación señala "carecen de cualquier tipo de privacidad, es decir, es de acceso totalmente público y accesible a cualquier usuario de internet". Por lo tanto, una vez identificados los autores de estos comentarios y justificada como lícita su detención, pasa a ser necesaria una autorización judicial para continuar con acciones como la incautación y clonado de sus teléfonos móviles, con los que poder corroborar la autoría de los hechos imputados.

Cuando hablamos de canales abiertos, nos referimos a todos los datos disponibles al público que encontramos en internet, independientemente de su ubicación geográfica. En el artículo 32 del Convenio de Budapest, se especifica que una parte podrá acceder a datos informáticos almacenados, sin autorización de la otra, cuando éstos provengan de una fuente abierta, por lo tanto accesible al público, independientemente de la ubicación geográfica..

El mero acceso a internet crea una serie de rastros o pistas que abandona el delincuente, siendo éstas dirigidas a un público anónimo, de manera más o menos camuflada. Por lo tanto, cuando son insertados elementos en la red, pudiendo éstos ser accesibles por cualquier usuario, se concurre un consentimiento tácito, excluyéndose así la posibilidad de afectación del derecho a la intimidad (art. 18.1 CE) así como al de protección de datos personales (art. 18.4 CE)[97].

Es por ello que podemos afirmar que la red, en términos generales, cuando nos encontremos en canales abiertos, no es considerada un espacio íntimo ni privado, siempre y cuando los datos se almacenen de forma lícita y cumplan con los requisitos de

[97] "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

la Ley de Protección de Datos[98]. Tampoco es considerado este escenario como protegido por el derecho al secreto de comunicaciones (art 18.3 CE), ya que aunque se produce una comunicación entre emisor y receptor o receptores, son éstos últimos personas indeterminadas para quien se comunica a través de este medio, y si no se exige una identificación previa que pueda ser verificada por parte de los usuarios, se entiende que existe un consentimiento tácito a que cualquiera puede acceder a estas mismas comunicaciones.

Así se pronuncia a este respecto la STS 752/2010, de 14 de julio, que ya antes de la modificación de la LECrim, afirma: "en relación con la vulneración del derecho al secreto de las comunicaciones, no aporta dato alguno fuera de identificarla con la captación de los mensajes y contactos realizados por el mismo a través de internet, olvidando que el acceso a la información así producida puede efectuarla cualquier usuario, no precisándose autorización judicial para conseguir lo que es público cuando el propio usuario de la red ha introducido dicha información en la misma (ver STS 739/2008 y las citadas en la misma)".

Por lo tanto, la navegación por espacios públicos, sin acceso a foros donde sea necesaria una previa identificación verificada, no encontrándose la investigación centrada en personas concretas a las que se pretenda engañar de forma deliberada, no debe plantear ningún problema.

Como ARRABAL PLATERO indica, no estarían vulnerándose los derechos fundamentales de los ciudadanos (como el de la intimidad, protección de datos o autodeterminación informativa), cuando se obtienen datos de libre acceso que el propietario a cedido o divulgado libremente en la Red[99].

Se incluyen dentro de canales abiertos las redes sociales, siempre que la misma no se utilice como canal de comunicación por parte del agente policial con el posible delincuente. Aunque podríamos llegar a la conclusión de que, realizando un registro en

[98] DELGADO MARTÍN, J., "Investigación y prueba de la piratería digital" *Diario La Ley*, julio 2020, p.11

[99] ARRABAL PLATERO, P., "La prueba tecnológica: aportación, práctica y valoración" Tirant Lo Blanch, Valencia, 2020, pp.206-209.

una red social, se entraría a un espacio privado, bien es cierto que este registro es un mero trámite, en el cual los datos personales no son obligatoriamente solicitados, ni tan siquiera la necesidad de que éstos sean reales, ya que no se requiere una verificación de los mismos.

El ciberpratullaje es, por lo tanto, una actuación de prevención y vigilancia de hechos ilícitos en la red, que se lleva a cabo en canales abiertos de comunicación, no atentando contra los derechos fundamentales de los usuarios de los mismos. Estas actuaciones podrían ser: el acceso a chats, entablar conversación con un supuesto delincuente no habiendo indicios claros de su actividad ilícita, establecer una comunicación estable en el tiempo cuando se tienen sospechas de una supuesta actividad ilegal e incluso recibir archivos ilícitos de otros usuarios.

Son diversas las sentencias que hacen referencia a estas actuaciones, como la STS 752/2010[100], que ya antes de la reforma de la LECrim indicaba que, el ciberpatrullaje "puede efectuarlo cualquier usuario, no precisándose autorización judicial para conseguir lo que es público cuando el propio usuario de la red ha introducido dicha información en la misma".

Como expresa ZARAGOZA TEJADA, no siempre es fácil discernir el momento exacto de la investigación a partir del cual es necesario acudir a esta figura[101]. Las situaciones especificas de cada investigación necesitan de una continua revisión de las diferentes actuaciones a llevar a cabo.

Cuando un agente policial interactúa con otros usuarios en la red bajo una identidad diferente de la real (refiriéndonos al uso de un pseudónimo o *nickname* falso), podría llevarnos a pensar que se está actuando como agente encubierto informático. Si bien es cierto que se está actuando bajo una identidad ficticia, cabe destacar que es precisamente el *modus operandis* habitual por parte de los usuarios de estos canales, entendiéndose por lo tanto que, las personas que interactúan a través de los mismos tienen pleno conocimiento de ello.

[100] STS 752/2010, de 14 de julio, de 2010.
[101] ZARAGOZA TEJADA, J.I., "El agente encubierto…Op.Cit. p.201-202

La jurisprudencia reconoce que el agente policial puede utilizar un *nickname* falso, no produciéndose engaño alguno, ya que es considerada una regla de uso general, la utilización de pseudónimos en la red. Por tanto, no será necesaria la autorización judicial previa al uso de un *nickname* falso, tal y como se expone en la STS 173/2018, de 11 de abril[102].

Cabe aquí destacar otras medidas de investigación tecnológica, como son los datos en poder de proveedores de servicios.

Entendemos por prestadores de servicios a las personas físicas o jurídicas que presten: servicios de comunicaciones electrónicas (como acceso a internet o de comunicaciones interpersonales), servicios de la sociedad de información (servicio prestado vía electrónica, a petición de un destinatario de servicios y normalmente a cambio de una remuneración) o servicios de asignación de nombres de dominio de internet y de direcciones de IP (proveedores de direcciones de IP, registradores de nombres de dominio, servicios de privacidad y representación).

Los proveedores de telecomunicaciones deberán disponer de los datos de abonado sus clientes. La Policía Judicial o el Ministerio Fiscal, podrán solicitar los datos de abonado sin necesidad de orden judicial para fines de investigación criminal, estando regulado en el artículo 588 ter m) Identificación de titulares o terminales o dispositivos de conectividad, de la Ley de Enjuiciamiento Criminal[103].

Estos datos de abonado serán los relativos a la identidad del cliente (nombre, dirección, teléfono, email, facturación, etc.) y al tipo de servicio contratado o duración del mismo. Serán con otros datos más precisos con los que sí será necesaria una autorización judicial, como veremos en el siguiente apartado.

En lo referente a la solicitud de datos, contamos con la reciente Ley Orgánica 7/2021,

[102] DELGADO MARTÍN, J., "Investigación y… Op. Cit… p.12.
[103] "Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia".

de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales[104]. Con esta normativa se pretende que los datos tratados por las autoridades competentes cumplan con los fines previstos, preservando los derechos fundamentales de los ciudadanos de la Unión Europea[105].

En su artículo 7, sobre el deber de colaboración, se especifica que tanto las administraciones públicas como cualquier persona física o jurídica, deberá facilitar los datos, informes, antecedentes o justificantes que le sean solicitados por la Policía Judicial, siempre que ésta cumpla con la justificación necesaria para el desarrollo de sus investigaciones. No será informado el interesado de la trasmisión de sus datos, para así garantizar la actividad investigadora. Estos datos podrían ser personales (nombre, DNI, datos de localización, identificador en línea, etc.) como biométricos, que faciliten la identificación inequívoca de una persona física.

Una vez se han reunido elementos suficientes que prueben la existencia de hechos ilícitos, siendo éstos suficientes para considerar la apertura de una investigación judicial definida, es cuando ha de ponerse en conocimiento de la autoridad judicial y solicitar la autorización de la misma para actuar bajo la figura de agente encubierto informático. Por lo tanto, teniendo en cuenta la normativa jurídica y la jurisprudencia existente, se determina que no será necesaria una orden judicial en las investigaciones de inteligencia procedentes de fuentes abiertas en internet.

Estas actuaciones podrían ser obtener la IP del investigado, la localización o posicionamiento de su IP, los nicks o redes sociales que usa, captación de conversaciones en chats o foros públicos, identificar terminales y números de abonado de los terminales identificados, solicitar datos bajo el amparo de la ley de protección de datos, interceptaciones de comunicaciones en caso de urgencia por terrorismo, etc.

---

[104] Mediante esta Ley se incorpora a nuestro ordenamiento jurídico la Directiva (UE) 2016/680, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
La referencia normativa del ordenamiento español es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[105] conforme al artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea, al artículo 16.1 TFUE y al artículo 18.4 de la Constitución.

Una vez se hace necesaria la autorización del uso de esta figura, es cuando acciones como el intercambio de archivos ilícitos o limitaciones de derechos fundamentales (siempre cumpliendo con el criterio de proporcionalidad), quedan amparados por la ley y no se entienden como vulneración de la misma, quedando el agente de la policía judicial, exento de responsabilidad penal por estos actos.

He aquí uno de los motivos por los que, en mi opinión, sería necesaria una legislación más específica de esta herramienta de la Policía Judicial. Ya que el agente de la misma, en sus funciones como agente encubierto informático, podría encontrarse con que está a punto de traspasar la delgada línea que separa la necesidad o no de la autorización judicial, pudiendo afectar al transcurso de una investigación e incluso perjudicando la misma.

Podría ser interesante la creación de un protocolo de actuación específico, donde se asiente un método rápido y eficaz, que proporcione una tranquilidad al agente implicado así como garantice el cumplimiento de la debida protección de los derechos fundamentales del investigado.

1.2. ACTUACIÓN EN CANALES CERRADOS

Es con la introducción del apartado 6 del art.282 bis LECrim, donde se legaliza la actuación bajo identidad supuesta por parte de los agentes de la policía judicial, previa autorización del juez de instrucción, en las comunicaciones dentro de canales cerrados, completándose con el segundo párrafo, que prevé el intercambio y envío de archivos ilícitos por parte del agente, así como analizar los algoritmos de éstos[106]. Así como el

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

apartado 7 del art.282 bis LECrim, que lo autoriza a la obtención y grabación de imágenes en el ámbito privado[107].

Por lo tanto, pudiendo aplicarse esta figura complementariamente a cualquier ilícito penal en el que sea necesario el análisis de cualquier documento digital, así como la entrada y registro domiciliario y la intervención de ordenadores o elementos de almacenamiento de memoria, siempre y cuando se enmarquen dentro de los delitos de terrorismo, delitos cometidos en el seno de una organización criminal o delitos dolosos castigados con penas con un límite máximo de, al menos, tres años de prisión; o cualquier otro delito cometido a través de medios informáticos.

La razón de ser de esta reforma viene de la necesidad de combatir las redes de pederastas, que estaban emigrando de redes P2P hacia foros más restringidos y sofisticados, solventando así el problema del control policial, al encontrarse éstos órganos con una dificultad jurídica para considerar las comunidades cerradas de pederastas como organizaciones criminales[108].

Esta figura no está exenta de polémica, ya que al acotarse su uso en canales cerrados y dejando fuera de ello los canales abiertos, hay quien considera que se empuja a un acercamiento excesivo de esta figura al delincuente, como apuntaba BUENO DE MATA en el 2015, antes de la creación de la nueva Ley[109].

Se entiende que la facultad otorgada por el legislador a la hora de intercambiar archivos ilícitos se utiliza para contrarrestar este ámbito de actuación más reducido y se consiga una confianza que garantice la eficacia de la infiltración por parte del agente encubierto virtual.

[107] "7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio."
[108] CAROU GARCÍA, S., "El agente… Op. Cit., p.27.
[109] BUENO DE MATA, F., "Drones, virus espía y agentes encubiertos en la red: comentarios a las nuevas medidas de investigación tecnológica en la normativa procesal española" Ponencia presentada al XIX Congreso Iberoamericano de derecho e informática, Medellín 2015, pp.:14-17.

Al estar recogidas en la LECrim estas autorizaciones de actuación de manera genérica, puede llevar al agente policial a situaciones de inseguridad jurídica, algo que se podrá salvar con una autorización judicial previa, siempre cumpliendo con el principio de necesidad y proporcionalidad.

Si bien es cierto que para obtener dicha autorización previa, debe de estar verificada la existencia de actividad delictiva, encontrándose aquí con una diferencia en cuanto al patrullaje físico, que podría solventarse con acciones como un seguimiento en zonas públicas del investigado. En el terreno tecnológico, para conseguir esa verificación, puede llegar a ser necesario un acercamiento tal que ponga al agente policial en la tesitura de comenzar un contacto con la persona investigada, para ganarse su confianza y asegurar la posibilidad de infiltración, pudiendo darse la situación límite de encontrarse ante una solicitud de verificación de identidad o de intercambio de archivos por parte de los presuntos delincuentes, que en caso de no ser resuelto de manera rápida, podría tener consecuencias negativas para la futura investigación.

Quienes rechazan esta facultad, matizan que no creen que deba existir el engaño a cualquier precio, incluso con un presunto delincuente. Además, la facultad del intercambio de archivos ilícitos podría llevar a la defensa del investigado a alegar una inducción al delito por parte del agente policial judicial, propio de la figura del agente provocador anteriormente definido, así como de uso de la comisión de delitos como herramienta de investigación.

Se ha planteado la posibilidad de utilizar material delictivo de antiguas redadas, aunque BUENO DE MATA argumenta que se estaría así menoscabando los derechos de las víctimas y seguiría cometiéndose por parte de los agentes un hecho punible[110]. Otra alternativa sería la de intercambiar material camuflado *ad hoc*, como sería el intercambio de material pedófilo en el cual apareciesen actores haciéndose pasar por menores de edad, o la creación de amenazas en redes sociales que se dirijan a personas ficticias, para así crear confianza con los sujetos investigados.

[110] BUENO DE MATA, F., "Drones, virus espía y agentes… *Op.Cit*, p.17.

Cabe aquí hacer un inciso sobre lo que sería la Ingeniería Social, que serían una serie de pautas que aprenden y estudian los delincuentes para ganarse la confianza de sus víctimas, siendo éstas seleccionadas en muchos casos para asegurar el éxito en sus fines delictivos. En el reciente Real decreto 43/2021 encontramos la definición de Ingeniería Social como "técnicas que buscan la revelación de información sensible de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima" [111].

Algún ejemplo de ingeniería social en el entorno tecnológico son esos emails en los que los remitentes se hacen pasar por la entidad bancaria del receptor, pidiendo que se acceda a un enlace y se faciliten ciertos datos de la cuenta, como podría ser la contraseña, y así poder hacerse con el control de la misma. Esto viene siendo una evolución de timos como el de la estampita [112] o quienes haciéndose pasar por inspectores del suministro del gas, expiden facturas falsas para cobrar a su víctima o con la excusa de comprobaciones en la vivienda, aprovechan para robar en su interior, principalmente siendo sus víctimas personas de edad avanzada.

Con el avance de las tecnologías, los delincuentes han adaptado estas estafas a otras más rentables por medio de las tecnologías, ya que, por ejemplo, en las estafas a través de la red pueden conseguir cantidades mayores de dinero que en un robo con violencia o un hurto, siendo la pena menor, al no considerarse el agravante violento. Dentro de las TIC, podemos tomar como ejemplo el phising, los secuestros virtuales o los engaños mediante chats que utilizan los pederastas para obtener fotografías o citas personales con menores de edad[113].

Los funcionarios de las diferentes unidades de información y policía judicial, especialmente aquellos agentes que actúen como agente encubierto informático, deben adoptar también esta ingeniería social, para conocer las técnicas que habitualmente

[111] RD 43/2021, de 26 de enero de 2021, que tiene como objetivo el de "dar una respuesta efectiva a los problemas de seguridad de las redes y sistemas de información…"
[112] Tradicional estafa que solía realizarse en España a principios del siglo XX, consiste en hacer que el estafado acepte una gran cantidad de supuestos billetes de alto valor a cambio de una cantidad de dinero más fraccionado.
[113] Real Decreto 43/2021, 2021), definición, <<*Phishing*>>: estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta empleando métodos de ingeniería social.

utilizan este tipo de delincuentes, usando el engaño como medio a la hora de delinquir en la red y asegurando así el éxito en su infiltración entre estas personas.

Podemos decir que una característica importante a la hora de trabajar como agente encubierto informático sería, precisamente, reproducir los patrones de actividad de los delincuentes virtuales, para hacer ver más real una cuenta personal a la hora de interactuar en su terreno. Por ejemplo, una cuenta personal en redes sociales, no puede seguir un patrón de actuación en horario de oficina.

Por lo tanto, creo que queda patente que para llevar a cabo la protección de la seguridad ciudadana, hay que tomar el ciberespacio como un nuevo escenario, y la prevención y el seguimiento de las personas con intención de delinquir en la red es imprescindible, así como una especial regulación.

Con la introducción del ya mencionado apartado 6, del artículo 282 bis de la LECrim y su mención a la posibilidad de "…analizar los resultados de los algoritmos…", se soluciona la posibilidad de utilizar un *"HASH"* por parte de los funcionarios de la Policía Judicial, algo muy utilizado actualmente, sobretodo con dos funcionalidades, la de proteger la cadena de custodia y la del uso de metadatos.

El "*HASH"* es una clave alfanumérica que se obtiene mediante el análisis de los contenidos de cualquier archivo informático. Su especificidad es tan alta que cualquier mínimo cambio en el contenido de un archivo determinaría la modificación de ese resultado[114].

La cadena de custodia es de vital importancia en cualquier investigación o actuación policial y es al poder realizarse sobre cualquier ordenador u otro elemento de almacenamiento de memoria un algoritmo "*HASH",* cuando se consigue obtener una huella dactilar que podrá ser usada más adelante por parte de la administración de justicia sobre los objetos intervenidos o sus copias de seguridad, para poder comprobar que lo analizado procede de lo intervenido sin género de dudas.

[114] Para más información, acudir a LÓPEZ ESPÍ, JL., SANCHEZ MONTERO, R., "Comentarios sobre la introducción al hash como técnica de seudonimización de datos personales de la AEPD" La Ley Privacidad, nº5, 2020.

La aplicación del algoritmo "*HASH"* sobre los metadatos concretos de fotografías o documentos, que son especialmente utilizados en las investigaciones referentes a la pornografía infantil, facilita la búsqueda de copias de éstos elementos en diferentes ordenadores de los investigados, pudiendo así establecerse una relación entre ellos[115]. Lo que se pretende es la posibilidad de identificar inequívocamente los archivos ilícitos que se han enviado o intercambiado[116].

Es por lo tanto necesario que las técnicas de investigación de la policía judicial y el agente encubierto informático en particular, sean técnicas que necesiten de una regulación y control, a través de un mandamiento judicial. Para entender en que supuestos sería necesaria la autorización judicial, podemos acudir a literatura como la de ARRABAL PLATERO[117], que los detalla en profundidad.

Con la interceptación de las comunicaciones telefónicas y telemáticas, reguladas en el artículo 588 ter a-i de la LECrim, se podrá tener acceso a tres tipos de datos: el contenido de la comunicación (requiere de autorización judicial o de debida urgencia, valorada y acreditada a posteriori judicialmente), los datos de tráfico (como podrían ser la fecha o duración de una comunicación) y los datos de abonado o conexión (existentes incluso cuando no existe la comunicación).

La LECrim reconoce la identificación de usuarios, terminales y dispositivos de conectividad[118], permitiendo la obtención de la identificación del usuario de una IP, del usuario de un terminal, o numeraciones de abonado de un dispositivo móvil.

---

[115] RD 1708/2011, 2011), definición, Metadato: "Se entiende por metadato cualquier descripción estandarizada de las características de un conjunto de datos. En el contexto del documento electrónico cualquier tipo de información en forma electrónica asociada a los documentos electrónicos, de carácter instrumental e independiente de su contenido, destinada al conocimiento inmediato y automatizable de alguna de sus características, con la finalidad de garantizar la disponibilidad, el acceso, la conservación y la interoperabilidad del propio documento ".

[116] Informe del Consejo Fiscal, Anteproyecto de Ley Orgánica de Modificación de la Ley de Enjuiciamiento Criminal parala agilización de la Justicia Penal, el Fortalecimiento de las Garantías Procesales y la Regulación de las Medidas de Investigación Tecnológicas, FISCALIA GENERAL DEL ESTADO, CONSEJO FISCAL, Madrid, 23 de enero de 2015, pp.26 y 27

[117] ARRABAL PLATERO, P., "La prueba… Op.Cit., pp.209-241.

[118] regulados con los artículos 588ter k) a 588 ter m) de la Lecrim

Un ejemplo de intento de equilibrio en cuanto a garantías constitucionales, podría ser lo regulado en la LECrim con respecto a la definición de límites cronológicos en la interceptación de las comunicaciones telefónicas o telemáticas[119]. La autorización de esta medida será efectiva por espacio de tres meses, prorrogables por períodos de igual duración, hasta dieciocho meses, siempre que subsistan la causas que motivaron dicha intervención[120]. Todo ello es importante a efectos de licitud de las pruebas obtenidas.

En el artículo 588 quater a-e, se regula la captación y grabación de comunicacioness orales mediante la utilización de dispositivos electrónicos.

También queda regulada la utilización de imágenes en lugares o espacios públicos, y además, será en ocasiones necesario el control remoto, seguimiento y localización del sujeto investigado, pudiendo realizarse por ejemplo, con un sistema de localización GPS. Todo ello regulado en el artículo 588 quinquies a-c.

Además, podríamos encontrarnos en el supuesto de que, en una investigación que ya cuenta con autorización del uso del agente encubierto informático, se solicite una autorización de entrada y registro. Una vez realizado el registro, estando los agentes de la Policía Judicial en posesión de sistemas informáticos físicos, se contempla la necesidad de acceder a información contenida en los mismos e incluso a información remota, como podría ser la contenida en una nube, siendo ésta accesible desde el dispositivo anteriormente citado.

Así, el registro de dispositivos de almacenamiento masivo de información, queda regulado por el artículo 588 sexies de la Lecrim. Dice su apartado a) la necesidad de una motivación individualizada por parte de la autoridad judicial para el acceso a los dispositivos que se pudieran incautar en un registro domiciliario. En el apartado b), se extiende esta exigencia a los dispositivos electrónicos que sean incautados fuera del

[119] Venía siendo parte de numerosas críticas por parte de doctrina y jurisprudencia, lo legislado en la Ley Orgánica 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, que con respecto a la limitación temporal de la medida de interceptación de las comunicaciones telefónicas, autorizaba a llevar a cabo la misma por períodos de tres meses, prorrogables por iguales períodos. Así, en el anterior artículo 579.3 LECrim, resaltaba la insuficiencia de regulación sobre el plazo máximo de prórrogas, que se entendía inexistente.

[120] Artículo 588 ter g, de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECRIM.

domicilio del investigado. Nombra el apartado c) las especificaciones sobre la autorización judicial.

El registro remoto sobre equipos informáticos se regula en el artículo 588 septies de la Lecrim. Este registro remoto se efectuará sin el consentimiento del sujeto investigado, siendo posible mediante instalación de software, el uso de códigos o datos de identificación para el acceso a los contenidos, o la instalación de un *keylogger*[121]. Estando acotado este supuesto a ciertos delitos, como los cometidos en el seno de una organización criminal, los delitos de terrorismo, delitos contra menores o personas con capacidad modificada judicialmente, delitos contra la Constitución, de traición y relativos a la defensa nacional[122].

El artículo 588 septies a, expone que la resolución judicial será debidamente motivada y muy específica en lo referente a los dispositivos a los que se extiende dicha autorización de registro remoto, el alcance de la misma, los agentes autorizados a su ejecución, así como la autorización de realizar copias de los datos informáticos.

En el artículo 588 septies b se expone que los prestadores de servicios y las personas señaladas en el artículo 588 ter e de la Lecrim, tendrán un deber de colaboración con las autoridades judiciales y los agentes de la policía judicial que les soliciten los datos e información necesaria.

La duración de esta medida tendrá un plazo de un mes, prorrogable por períodos de la misma duración, hasta un máximo de tres meses, tal y como expone el artículo 588 septies c. Esta limitación tan reducida a mi entender es una garantía constitucional a los derechos del investigado, porque se ha querido proteger el mencionado anteriormente derecho a la identidad virtual, debido a que estaríamos contemplando la posibilidad de acceso a todo tipo de datos.

[121] Definición de *Keylogger* extraída de la lectura "*What´s a keylogger? The working principles, main features and use cases*" de la web www.keylogger.com: "instrumento que almacena las pulsaciones específicas que se realizan en el teclado de un dispositivo, a través de un hardware o software, memorizándolas posteriormente en un fichero o pudiendo ser éstas enciadas a través de internet."
[122] Art.588 *septies* a) de la Lecrim.

2. RESPONSABILIDADES DERIVADAS DEL AGENTE ENCUBIERTO

Se prevé que el agente encubierto informático, para infiltrarse con éxito dentro de comunidades u organizaciones criminales, deberá llevar a cabo actuaciones ilícitas con el fin de pasar desapercibido en estos escenarios.

Estará exento de responsabilidad únicamente en las actuaciones en las que se cuente con la autorización por parte del juez de instrucción que garantice el uso de esta figura como una consecuencia necesaria en el transcurso de la investigación y quede justificada la protección de los derechos fundamentales del investigado.

Por lo tanto, de presentarse una extralimitación en sus funciones, se incurrirá en una acción ilícita que podrá dar lugar a responsabilidades penales, civiles o disciplinarias.

La extralimitación puede ser una línea muy delgada en el ámbito de la infiltración virtual, por lo que creo necesario valorar paso a paso las pautas a seguir en cada investigación, así como tener una comunicación frecuente con las autoridades judiciales, siendo lo más conciso posible en los informes internos.

2.1. PENAL

El art. 282 bis de la LECrim, se especifica en el apartado 5 que será exento de responsabilidad criminal el agente de la policía judicial por los actos que hayan sido cometidos durante su investigación, siendo éstos considerados una consecuencia necesaria en el desarrollo de la misma y no constituyendo una provocación al delito, siempre guardando la debida proporcionalidad. Como dice PERALS CALLEJA, este precepto no es una "carta en blanco", sino que se establece una limitación[123].

Siendo el principio de proporcionalidad, un principio presente en el artículo 25 de la Constitución, que debe respetarse a la hora de adoptar cualquier medida que afecte a un

[123] PERALS CALLEJA, J., "El agente encubierto, la figura del arrepentido. Protección de testigos. Entrada y registro. Apertura de correspondencia", Cendoj, 2010, p. 10.

derecho fundamental, y como ZAFRA ESPINOSA señala, siendo éste un mecanismo de control que "limite la actuación arbitraria de los poderes públicos" [124].

Este principio de proporcionalidad, así como los principios rectores mencionados en el artículo 588 bis a, (especialidad, idoneidad y necesidad) por los cuales debe regirse la autorización judicial, está directamente relacionado con la responsabilidad penal del agente encubierto informático, debiendo éste respetarlo no sólo con el fin de comenzar una investigación, sino también durante toda su intervención[125].

Por lo tanto, el agente encubierto informático no debe olvidar que la autorización judicial inicial, no lo exime de una responsabilidad en la totalidad de su actuación, sino que deberá estar en continua revisión por parte del juez y respetar en todo momento estos principios rectores.

Se hace referencia en el apartado 1 del artículo 282 bis, los supuestos en los que existe una previsión legal de las conductas del agente, como serían el actuar bajo identidad supuesta, adquirir, transportar, así como diferir la incautación de los objetos, efectos e instrumentos del delito.

El agente de la policía judicial, en el supuesto de incurrir en la comisión de delitos en el momento previo a la autorización judicial, no estará protegido por esa exención de responsabilidad prevista en el apartado 5.

Cuando se persigue criminalmente a un agente encubierto informático, se pueden aplicar atenuantes o eximentes, como podrían ser la legítima defensa o estado de necesidad. Así viene recogido en el artículo 20.7 del Código Penal, aplicándose esa exención al actuar dicho agente "en cumplimiento de un deber o en el ejercicio legítimo de un derecho, oficio o cargo".

Y como requisitos para imputar y posteriormente juzgar al agente encubierto, esto deberá decidirse en un proceso penal independiente y será obligatorio un informe del

[124] ZAFRA ESPINOSA DE LOS MOTEROS, R., "El policía infiltrado, los presupuestos jurídicos en el proceso penal español". *Tirant lo Blanch,* Valencia 2.010, p.370.
[125] ZAFRA ESPINOSA DE LOS MOTEROS, R., "El policía infiltrado… Op. Cit. p.372.

órgano que autorizó dicha infiltración, siendo su elaboración previa un requisito imprescindible a la hora de atribuir o no esa responsabilidad al agente encubierto informático[126].

2.2. CIVIL

Como explica ASENCIO MELLADO, la responsabilidad civil, estando conexa con lo anterior, no debe confundirse de la responsabilidad penal[127]. Es acumulable la pretensión penal a la pretensión civil, al igual que en otros procesos penales, y cuando un delito produce un daño de naturaleza civil, debe ser asumida por los causantes del daño o de quien ha aceptado tal responsabilidad. Dicha responsabilidad puede dividirse en dos tipos, contractual o extracontractual.

El artículo 100 de la LECrim señala que "de todo delito o falta nace acción penal para el castigo del culpable, y puede nacer también acción civil para la restitución de la cosa, la reparación del daño y la indemnización de perjuicios causados por el hecho punible". y 116 del Código Penal. "Toda persona criminalmente responsable de un delito lo es también civilmente si del hecho se derivaren daños o perjuicios."

El artículo 1911 del Código Civil nos dice que "del cumplimiento de las obligaciones responde el deudor con todos sus bienes, presentes y futuros".

El Código Penal, en su artículo 121, establece la responsabilidad del Estado cuando se produzcan daños calificables de civiles. Esta responsabilidad surge cuando los hechos cometidos sean por parte de una autoridad, agentes, contratados o funcionarios en dependencia de la Administración, habiendo sido cometidos en el ejercicio del cargo o función.

[126] ZAFRA ESPINOSA DE LOS MOTEROS, R., "El policía infiltrado… Op. Cit. pp.424 y 425.
[127] ASENCIO MELLADO, JM., "El agente encubierto", en *Derecho procesal penal* (Coord. FUENTES SORUANO, O.), Tirant lo Blanch, Valencia, 2020, p.91.

Por lo tanto, se entiende que surge la responsabilidad civil contractual del agente encubierto virtual cuando, actuando bajo una identidad supuesta, realiza una serie de actos o negocios jurídicos, no siendo éstos necesarios para llevar a cabo la investigación. Se entiende por responsabilidad civil extracontractual como aquella que deriva de la comisión de un ilícito penal, estableciendo el artículo 1902 del Código Civil que "el que por acción u omisión cause daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado".

Por lo tanto, si la responsabilidad civil del agente encubierto informático no viene de una conducta necesaria y proporcional a la investigación en curso, éste responderá frente al estado y terceros perjudicados, siendo el Estado subsidiariamente quien se haga cargo de esa indemnización a terceros cuando el agente no indemnice el daño causado[128].

2.3. DISCIPLINARIA

El agente encubierto informático, siendo un agente de la Policía Judicial, está sometido al régimen de responsabilidad de los funcionarios públicos, y como se dispone en el artículo 10 de la LO 4/2010, de 20 de mayo, de Fuerzas y Cuerpos de seguridad del estado, se considera cualquier conducta constitutiva de un delito doloso como falta muy grave, siendo éstas sancionadas con la separación del servicio, la suspensión de sus funciones de tres meses y un día a seis años, o el traslado forzoso[129].

Se pronuncia CARDOSO PEREIRA con respecto a este régimen, expresando que no hay una corriente de única interpretación, ya que la sanción administrativa viene vinculada a la resolución del proceso penal, pudiendo entenderse como una infracción del principio "non bis in idem", que anularía la sanción anterior[130].

[128] ZAFRA ESPINOSA DE LOS MOTEROS, R., "El policía infiltrado… Op. Cit. p.422.
[129] Disponible en: https://www.boe.es/eli/es/lo/2010/05/20/4/con
[130] CARDOSO PEREIRA, F., "Agente encubierto en el proceso penal garantista: Límites y desafíos", *Tesis doctoral, Universidad de Salamanca*, Salamanca 2012, p. 312- 319.

Este principio consiste en no castigar a la misma persona más de una vez por la comisión de un mismo hecho punible o delito. Aunque este principio eximiría de la sanción administrativa a cualquier persona, la condición de funcionario y su sujeción especial con la Administración, hace posible la doble sanción penal y administrativa de un mismo hecho.

Esta doble sanción se justifica por sus diferentes fundamentaciones. Se entiende que penalmente se responde como ciudadano, y administrativamente como persona de relación especial, en la que se ha quebrado la relación de confianza otorgada por el Estado. Ahora bien, si la infracción penal ya contempla esta relación especial, el principio "non bis in idem" sí que sería aplicado[131].

Desde mi punto de vista, la condición de funcionario de la Administración, no es motivo suficiente por el que sancionar doblemente, ya que el castigo es mucho mayor en comparación con el que se aplicaría a cualquier otro ciudadano.

[131] Para ampliar conocimientos sobre el principio "non bis in idem", acudir a la STC 2/2003, STC 159/1985 y STC 77/1983

CONCLUSIONES

Tras la lectura, estudio y análisis de nuestra legislación, jurisprudencia y diferentes artículos, he podido profundizar en la figura del agente encubierto informático, llegando a una serie de conclusiones, las cuales me dispongo a enumerar.

Primera. - Es un deber de nuestras fuerzas y cuerpos de seguridad, así como del legislador, el garantizar ese respeto a los derechos fundamentales de cualquier ciudadano, resultando imprescindible el control judicial, tal y como se exige, en las investigaciones en las que el agente encubierto informático va a ser utilizado como medida investigativa.

Segunda. - El auge de los delitos informáticos crea la necesidad de unas leyes que, dentro de lo posible, avancen en paralelo e incluso se adelanten a las necesidades de nuestra actualidad, que no den lugar a vacíos legales que impidan una correcta investigación, garantizando la eficiencia de la misma. Siendo necesaria la colaboración con expertos de la materia, que puedan llevar a cabo una mejor tasación de los delitos y la inclusión de nuevos términos delictivos.

Tercera. - Resaltar la inseguridad jurídica a la que pueden enfrentarse los agentes de la policía judicial, ya que los límites de su actuación como agente encubierto informático están redactados de manera genérica, dependiendo de la discrecionalidad judicial, en ocasiones, con unas líneas muy delgadas. Requiere de especial atención el envío de archivos ilícitos, que puede derivar en una nulidad de las actuaciones, ya que podría llegar a entenderse como una provocación. Es por ello que creo necesaria una regulación más solida , que no deje lugar a dudas ante la escasez o ambigüedad de la misma.

Cuarta. – Creo necesario trabajar en una normativa común para las diferentes unidades de Policía Judicial de nuestro país. Dada la diversidad de cuerpos policiales, unificar protocolos concretos de actuación y colaboración. Trabajar especialmente en criterios y códigos de conducta comunes para delitos más sensibles, como el terrorismo o la pedofilia.

Quinta. - Las competencias para la actuación como agente encubierto informático son exclusivas de la Policía Judicial, creo que debería dotarse a todo cuerpo policial, independientemente de su dependencia territorial, de la formación y medios necesarios para contar con dicha especialidad.

BIBLIOGRAFÍA

ALCOLADO CHICO, M.T., "La evolución hacia la moderna funcionalidad del "agente encubierto": incidencia de las nuevas reglas de la ley de enjuiciamiento criminal" *Revista jurídica de Asturias* Madrid, 2016, nº39.

ARRABAL PLATERO, P., "El derecho fundamental al propio entorno virtual y su incidencia en el proceso", en *Era Digital, Sociedad y Derecho* (Dir. FUENTES SORIANO; Coords. ARRABAL PLATERO, DOIG DÍAZ, ORTEGA GIMÉNEZ, TURÉGANO MANSILLA), Tirant Lo Blanch, Valencia, 2020, pp. 431-441.

ARRABAL PLATERO, P., "La prueba tecnológica: aportación, práctica y valoración" Tirant Lo Blanch, Valencia, 2020.

ASENCIO MELLADO, JM., "El agente encubierto", en *Derecho procesal penal* (Coord. FUENTES SORUANO, O.), Tirant lo Blanch, Valencia, 2020.

BILLINGSLEY, R.; NEMITZ, T. y BEAN, P.; «Informers: policing, policy, practice», Ed. Willan, Oregón, 2001.

BUENO DE MATA, F., "Drones, virus espía y agentes encubiertos en la red: comentarios a las nuevas medidas de investigación tecnológica en la normativa procesal española" Ponencia presentada al XIX Congreso Iberoamericano de derecho e informática, Medellín 2015.

CARDOSO PEREIRA, F., "Agente encubierto en el proceso penal garantista: Límites y desafíos", *Tesis doctoral, Universidad de Salamanca*, Salamanca 2012.

CAROU GARCÍA, S., "El agente encubierto como instrumento de lucha contra la pornografía infantil en internet" Cuadernos de la Guardia Civil, Revista de Seguridad Pública nº 56, 2018, disponible en: https://www.guardiacivil.es/es/institucional/Cuadernos_de_la_Guardia_Civil/index.html

CUADRADO SALINAS, C., "La Policía Judicial", en *Derecho procesal penal* (Coord. FUENTES SORUANO, O.), Tirant lo Blanch, Valencia, 2020.

DE LA CUESTA ARZAMENDI, J. L. (DIR.)/DE LA MATA BARRANCO, N. J. (COORD.):Derecho penal informático, Civitas, Cizur Menor, 2010.

DEL POZO PÉREZ, M., "El agente encubierto como medio de investigación de la delincuencia organizada den la Ley de Enjuiciamiento Criminal española", *Revista Criterio Jurídico*, vol.6, 2006.

DELGADO MARTÍN, J., "Investigación y prueba de la piratería digital" *Diario La Ley*, julio 2020.

DELGADO MARTÍN, J., *Criminalidad organizada*, J.M.Bosch Editor, Barcelona, 2001.

DÍAZ MAROTO Y VILLAREJO, J., "Algunos aspectos jurídico penales y procesales de la figura del arrepentido", *Diario La Ley*, nº 5, España 1996.

EXPÓSITO LÓPEZ, L., "El agente encubierto", *Revista de derecho, UNED,* https://doi.org/10.5944/rduned *nº*17, 2015.

GASCÓN INCHAUSTI GASCÓN INCHAUSTI, F. "Infiltración policial y agente encubierto", Comares, Granada, 2001.

GIMENO SENDRA, J.V., *Derecho procesal penal*, Editorial Civitas, Navarra, 2012.

GÓMEZ DE LIAÑO FONSECA HERRERO, M., *Criminalidad organizada y medios extraordinarios de investigación*, Cólex, Madrid 2004.

HARFIELD, C.; "Police informers and professional ethics", *Criminal Justice Ethics*, vol.31, n.º2, https://www.tandfonline.com/doi/abs/10.1080/0731129X.2012.696960 2012.

LAFONT NICUESA, L., "El agente encubierto en el proyecto de reforma de la Ley de Enjuiciamiento Criminal", Diario La Ley, núm. 8580, Julio 2015.

LÓPEZ ESPÍ, JL., SANCHEZ MONTERO, R., "Comentarios sobre la introducción al hash como técnica de seudonimización de datos personales de la AEPD" La Ley Privacidad, nº5, 2020.

LÓPEZ GARCÍA, E., "Agente encubierto y agente provocador, ¿dos figuras incompatibles?" *Diario La Ley*, 2003. Nº4.

LÓPEZ YAGÜES, V., "El agente encubierto", en *Derecho procesal penal* (Coord. FUENTES SORIANO, O.), Tirant lo Blanch, Valencia, 2020.

MARCHAL GONZÁLEZ, A.N., "Precisión terminológica en torno a la figura del confidente en el proceso penal", *Diario La Ley*, nº9083, España 2017.

MIRÓ LLINARES, F., "La oportunidad criminal en el ciberespacio: aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen." *Revista Electrónica de Ciencia Penal y Criminología.* https://dialnet.unirioja.es/metricas/documentos/ARTREV/4396388, noviembre 2011.

MITCHSON, N., URRY, R., "Delitos y abusos en el comercio electrónico". *The IPTS Report,* 2001, nº57.

MUÑOZ SÄNCHEZ; J:, *El agente provocador*, Monografías 36, Valencia 1995.

PERALS CALLEJA, J. "Técnicas de investigación del crimen organizado: el agente encubierto, confidente, regulación en España y validez de la prueba obtenida en el extranjero, problemas práctica de la heterogénea regulación de la materia", *Cuadernos digitales de formación*, 2010.

PERALS CALLEJA, J., "El agente encubierto, la figura del arrepentido. Protección de testigos. Entrada y registro. Apertura de correspondencia", Cendoj, 2010.

PÉREZ ARIAS, J., "Cibercriminalidad: hacia la nueva realidad virtual del derecho penal" *Revista Internacional de Doctrina y Jurisprudencia,* España 2021.

REDONDO HERMIDA, A., "El agente encubierto en la Jurisprudencia española y en la doctrina del TEDH", *La Ley Penal,* España, enero 2008.

SANCHEZ TOMÁS, J.M., *Derecho de las drogas y drogodependencias,* FAD, Madrid, 2002.

VALIÑO CES, A., "Una lectura crítica en relación al agente encubierto informático tras la Ley Orgánica 13/2015", Diario La Ley, núm. 8731, 2016.

VVAA, *The criminal law handbook: know your rights, survive…*, Ed. NOLO, Estados Unidos, 2011.

ZAFRA ESPINOSA DE LOS MOTEROS, R., "El policía infiltrado, los presupuestos jurídicos en el proceso penal español". *Tirant lo Blanch,* Valencia 2010.

ZARAGOZA TEJADA, J., "Investigación tecnológica y derechos fundamentales, comentarios a las modificaciones introducidas por la ley 13/2015. El agente encubierto online" Editorial Aranzadi, 2017.

ZARAGOZA TEJADA, J.I., "El agente encubierto online", en Investigación tecnológica y derechos fundamentales (Coord. ZARAGOZA TEJADA), Editorial Aranzadi, Navarra 2017.

ZARAGOZA TEJADA, J.I., "El agente encubierto online: la última frontera de la investigación penal", *Revista Aranzadi Doctrinal,* nº1, 2017.