EL AGENTE ENCUBIERTO INFORMÁTICO Y EL TERRORISMO

Jaime Camarero Arellano, Álvaro Greciano Sobrino,
Celia López Gil, Marta Mateo García,
Tiffany Martín Fernández, María Monteagudo Pose,
Cayetana Mosteiro Cadaval y Mayca Ndiba Nzang

Tutores: *Lorenzo M. Bujosa Vadell y Walter Reifarth Muñoz*

Universidad de Salamanca, España

Resumen

A lo largo de la historia se ha evidenciado que el terrorismo es un fenómeno nacional e internacional que necesita ser resuelto por parte de los Estados. Para ello, se han creado diversos mecanismos, entre los que destaca el agente encubierto informático, una figura que ha alcanzado una importancia destacable como respuesta al uso de la tecnología por parte de las organizaciones terroristas. En la presente ponencia caracterizaremos al agente encubierto diferenciándolo del agente provocador y analizaremos sus requisitos de actuación, así como la proyección internacional de esta herramienta procesal. Igualmente, examinaremos el tratamiento que reciben en el proceso las pruebas que este agente obtiene, sin olvidarnos de señalar los límites propios de un Estado de Derecho, que exigen una intervención informática encubierta que respete los derechos y las libertades fundamentales de las personas.

Abstract

Over the History, terrorism has shown to be a national and international phenomenon that needs to be confronted by States. To this end, many mechanisms have been created, among which, out stands the undercover computer agent. This figure has achieved remarkable importance in response to the use of technology by the terrorist

organizations. In this paper, we will characterize the undercover agent, differentiating it from the agent provocateur, and we will analyze the requirements for its action, as well as the international projection of this procedural tool. We will indeed examine the procedural treatment of evidence obtained by this agent and will finish by listing the limits established by the rule of law, which advocates for an undercover action respectful with fundamental rights and freedom.

1. Introducción

El literato Miguel de Unamuno defendía que el escritor no estaba obligado a ponerse al alcance del público, sino que era obligación de éste ponerse al alcance de aquel. Con todos nuestros respetos y la más alta consideración a este prócer de las letras hispanas, este equipo ha apostado, en cambio, por la realización de un texto sólido, pero accesible, que pueda ser utilizado en la investigación y que no por ello adolezca de una excesiva complejidad.

El tema de la exposición, el agente encubierto y el terrorismo, ha sido seleccionado por dos motivos: el primero, la carencia de producción científica sobre la materia, dado el relativamente reciente nacimiento de la figura; y el segundo, lo interesante del análisis de la traslación de una figura física al ámbito digital.

Sin embargo, a las dos motivaciones anteriores hay que añadir una tercera, de no menor importancia, esta es el estudio del terrorismo en una de sus múltiples vertientes. Lo novedoso de este instrumento se traduce en una falta de implementación en un número destacable de ordenamientos jurídicos; a pesar de ello, la legislación española, innovadora en este aspecto, sí que la incluye en sus leyes procesales.

Así, este escrito, realiza numerosas referencias a esta normativa pues abre la espita pudiendo servir como ejemplo a emular en la producción legislativa de otros países de su entorno o de su tradición histórica.

La investigación intenta abordar, de manera somera, los aspectos fundamentales que rodean al agente encubierto, con especial hincapié en las pruebas que éste pueda recabar y el tratamiento que reciben en el proceso. Ello no impide tratar otras cuestiones como el terrorismo en términos generales o el propio agente encubierto en particular. Entre estas no puede obviarse los posibles perjuicios que se pueden generar de la actuación del agente encubierto o la colaboración a nivel internacional entre los diferentes cuerpos policiales.

De esta manera se busca elaborar, en conjunto, un documento que proporciona las notas fundamentales sobre la labor del agente encubierto informático en la lucha contra el terrorismo. En todo caso, las páginas aúnan la investigación doctrinal con el análisis de la legislación y la jurisprudencia, aportando como

valor añadido una serie de valoraciones éticas cuyas implicaciones constituyen el trasfondo de este trabajo. Con ello, se pretende proporcionar al receptor del texto una serie de estímulos a lo largo de la lectura que sirvan, a su vez, para otorgar a la reflexión un carácter transversal y crítico.

2. El terrorismo como fenómeno nacional e internacional

Hablar de terrorismo es hablar de imágenes y sucesos que conmocionan a la opinión pública. En los últimos años, Barcelona 2017 (16 muertos), el atentado de Niza de 2016 (86 muertos), la masacre de París de 2015 (130 muertos), el 11 de marzo de 2004 en Madrid (con 193 víctimas) o el 11-S de 2001 con casi 3000 ciudadanos perdidos. Todos ellos perpetrados en lo que llamamos "Occidente" o "Mundo civilizado", pero en el resto del orbe han ocurrido muchos más de los que apenas hemos tenido constancia, sirve de ejemplo la Masacre de Camp Speicher en Irak, segundo acto terrorista más mortífero de la historia con más de 1900 víctimas reconocidas. Todas las masacres anteriores fueron perpetradas por diversas organizaciones que compartían la autoría islamista.

¿Significa esto que los únicos capacitados para perpetrar estas atrocidades son musulmanes? ¿O que todos los musulmanes son terroristas? Ambas preguntas se pueden atajar con un rotundo no. La historia mundial se ha visto marcada por numerosos actos terroristas, con mayor o menor impacto, con motivaciones muy variadas. Solo que cuanto más nos remontamos en el tiempo su poder de presión era menor al igual que la repercusión de sus actuaciones. Retrocediendo algo más de un siglo, podemos mencionar el asesinato del archiduque Francisco Fernando de Austria (1914) que originó de forma indirecta la Primera Guerra Mundial.

Atendiendo a los criterios de lo conocido como "terrorismo moderno", los atentados yihadistas son una de las últimas apariciones. Pero, antes de estos, existían otras acciones que, de seguir la línea únicamente lingüística, obedecerían a la acepción de terrorismo. Según la Academia:

> *Dominación por el terror; sucesión de actos de violencia ejecutados para infundir terror; actuación criminal de bandas organizadas, que, reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos*[1].

Para centrarnos en un mejor desarrollo de esta ponencia, únicamente hablaremos de organizaciones criminales y no de estados (incluiremos el Estado

[1] Definición de terrorismo según el diccionario de la Real Academia de Lengua Española (consultado por última vez el 18 de julio de 2021).

Islámico por ser únicamente un territorio ilegítimamente ocupado por una organización terrorista).

Por tanto, la primera manifestación de esta práctica tiene lugar en la antigua Judea, actual Israel, en el 1 a.C., Judas de Galilea fundo un grupo llamado Sicarii, dedicado en casi totalidad al asesinato de colaboradores de los romanos, sacerdotes, saduceos, herodianos y otras elites adineradas. Su forma de actuar era simple pero eficaz: mezclarse en la multitud en fiestas y aprovechar el caos para asesinar a sus objetivos. Una técnica todavía utilizada en actos combinados como Londres 2017 o Niza 2020.[2]

Avanzaremos casi veinte siglos hasta Irlanda, en 1858. La Hermandad Republicana Irlandesa realizó una serie de actos de creciente violencia en Gran Bretaña con el fin de infundir miedo y presión. El más importante fue en la prisión de Clerkenwell: para liberar a uno de sus cabecillas, realizaron una explosión de gran calibre con la que volaron parte del muro, llevándose por delante la vida de doce reclusos. Sus acciones fueron suficientes como para provocar la creación de la primera unidad antiterrorista de la historia. Fue conocida como la Rama Especial Irlandesa y se creó en 1883 por la Policía Metropolitana.

Llegamos a finales del siglo XIX, cuando los terroristas de carácter anarquista lograron cometer varios atentados políticos arrebatando la vida de decenas de políticos y figuras relevantes, entre los que destacan el presidente de la República Francesa Marie François Sadi Carnot (1894), del presidente del Consejo de Ministros español Antonio Cánovas del Castillo (1897) y de la emperatriz de Austria-Hungría, Isabel de Baviera (1898).

Una de las caras que pasan más desapercibidas al hablar de terrorismo es el estadounidense. Y si, quienes se erigen como máximos exponentes de la lucha contra el terrorismo, tienen un pasado algo más oscuro del que creemos. El Ku Klux Klan es a día de hoy, considerado por numerosos entendidos, como organización terrorista. Su carácter antisemita, supremacista blanco y anticomunista les otorgo un apoyo social abismal (en su apogeo se estima que tuvieron cinco millones de miembros), que dejó tras de sí un rastro de asesinatos de activistas, personas de color y disidentes[3].

En las postrimerías del siglo pasado, cabe reseñar una de las pocas organizaciones terroristas que lograron imponer sus ideales: el IRA. El ejército revolucionario irlandés estaba ubicado en la frontera entre un grupo revolu-

---

2 SÁNCHEZ LÓPEZ, V.: Terrorismo en el Alto Imperio Romano (43 a.C.-197 d.C.): semejanzas de un fenómeno moderno en tiempos antiguos. Tesis doctoral de la Universidad Complutense de Madrid, 2018.

3 BLANCO NAVARRO, J. M.; COHEN VILLAVERDE, J.: *Supremacismo blanco*. Instituto Español de Estudios Estratégicos (IEEE), Madrid, 2017, pp. 6-10.

cionario y una organización terrorista. Sus primeras tenían como objetivo la consecución de la independencia irlandesa de Reino Unido. Sus grupos paramilitares lucharon hasta la firma del Tratado Anglo-irlandés, donde se reconoció la independencia de la región, pero no de toda la isla[4]. Algunos de sus actos más crueles fueron los ataques simultáneos a 300 comisarías o la ejecución en masa de policías de Liverpool. Hay que realizar un apunte importante, y es que el IRA no es el actual ejército de Irlanda, conocido como Fuerzas de Defensa Irlandesa.

Su legado fue recogido por diferentes organizaciones. Una de las más conocidas es ETA que luchaba por la independencia del País Vasco cometiendo atentados, ejecuciones y diversas acciones de parecida índole. Pese a llevar algunos años con escaramuzas y asesinatos destaca por su relevancia el asesinato del presidente del Gobierno de España Don Luis Carrero Blanco (1973). Tras él, una larga lista que recorre décadas y deja un reguero de dolor, sangre y malestar social.

A día de hoy, la banda ha sido desmantelada, perseguida y muchos de sus cabecillas condenados por los tribunales. Su último atentado fue en 2009. En total, 853 muertos y 6389 heridos forman su haber delictivo. Casi todos fueron españoles, pero hubo pérdidas francesas, alemanas, estadounidenses y ecuatorianas, pues su método de acción fluctuaba de las intervenciones concretas (como el asesinato de Miguel Ángel Blanco) a los atentados en masa (el del supermercado Hipercor o la casa cuartel de la Guardia Civil de Zaragoza).[5]

Y, pese a que todas estas acciones son absolutamente condenables, y el tiempo otorgó a la justicia las acciones necesarias, España gestó para su lucha uno de los cuerpos más reprochables que ha habido nunca en la historia de la democracia: Los GAL. Los Grupos Antiterroristas de Liberación realizaron una "guerra sucia" o terrorismo de Estado contra ETA, combatieron atentados con más atentados[6]. En sus 4 años de historia perpetraron 30 atentados, aprendiendo y usando las técnicas del terrorismo vasco. Sin embargo, la justicia española

---

4 MCCARTNEY, C.: "Haciendo balance. El proceso de paz de Irlanda del Norte", en *Red Gernika Gogoratuz*, núm. 11, 2001.

5 Las cifras varían según la fuente consultada. Sin embargo, siempre se sitúan en el entorno de las aquí citadas. Con objeto de aportar unas cifras contrastadas se han utilizado diversas fuentes. Periódico *El País* https://elpais.com/politica/2018/05/02/actualidad/1525252299_953564.html y *El Correo Vasco* http://especial.elcorreo.com/2018/muertos-eta/. Al respecto también puede consultarse las bases del Ministerio del Interior español "Tabla de fallecidos por terrorismo indemnizados. Datos oficiales del Ministerio del Interior", *disponible en* http://www.interior.gob.es/fallecidos-por-terrorismo *(todos los enlaces han sido consultados por* última vez el 20 de julio de 2021).

6 PORTILLA CONTRERAS, G.: "Terrorismo de Estado: los grupos antiterroristas de liberación (G. A. L.)", en ARROYO ZAPATERO, L.; BERDUGO GOMEZ DE LA TORRE, I. (dir.): *Homenaje al Dr. Marino Barbero Santos in memoriam*. Ediciones de

supo obrar con imparcialidad y se falló condenando a estos grupos. De igual manera, se demostró que fueron financiados por el Ministerio del Interior, y se depuraron responsabilidades, produciéndose la dimisión de numerosos cargos gubernamentales. La actuación de los GAL nos muestra como algunos agentes encubiertos tomaron parte activa y, vulnerando todos los principios y reglas posibles, ejecutaban y secuestraban a quienes estimaran oportuno, provocando que algunas de sus víctimas fueran blancos erróneos y bajas colaterales. Lo anterior demuestra la importancia que se otorgó después a un correcto desarrollo de las misiones encubiertas y la vigilancia y control de los agentes; de entre estos uno de los más conocidos fue Mikel Lejarza, más conocido como "Lobo", quien en su actividad encubierta logró cercenar a toda la cúpula de ETA en 1975 y provocar la captura de otros 150 miembros.

Podemos afirmar con rotundidad que pudimos derrotar a ETA (cese definitivo en 2011) y que los GAL son cosa del pasado, pero su marca siempre quedará en la memoria colectiva española. A principios del presente siglo, una generación de nuestro país vivía con miedo diario a atentados de ETA, pero en 2004, se produjo una variación en la autoría de los atentados que la población española había sufrido hasta el momento. El 11 de marzo de 2004, 4 trenes explotaron en Madrid provocando la muerte de 193 personas y lesiones a 2000. Al Qaeda reivindicó el suceso como venganza al apoyo del gobierno a la invasión de Irak y Afganistán[7].

Para comprender mejor el alcance y los motivos de este suceso, debemos hacer un viaje en el tiempo al día 11 de septiembre de 2001, el día de inflexión en esta historia.

3000 personas fallecieron en lo que hasta hoy son los atentados más grandes de la historia. El terrorismo yihadista hizo su entrada en la historia. El yihadismo es un neologismo occidental que hace referencia a un tipo de ideología caracterizada por la frecuente y brutal utilización del terrorismo, en nombre de una pretendida yihad, a la cual sus seguidores llaman una «guerra santa» en el nombre de Alá. Se habla de pretendida yihad porque la yihad es un concepto básico del Islam.

El concepto tiene dos acepciones: la «yihad menor» que abarca dos conceptos: por un lado, la lucha militar en nombre de Dios contra un enemigo malvado y defendiendo una causa justa del lado del bien, concepto en el que

---

la Universidad de Castilla-La Mancha y Ediciones Universidad Salamanca, Cuenca, 2001, pp. 501-530.

7 PÉREZ VENTURA, O.: "Análisis del atentado del 11M" en PÉREZ VENTURA, O. (coord). *Curso avanzado sobre terrorismo yihadista en España*. CISDE-UDIMA, Madrid, 2012, pp. 13-14.

se intentan legitimar los yihadistas tergiversando el propósito original; y por otro lado cualquier acción realizada por Dios para mejorar la humanidad; y la «yihad mayor», de completa interpretación espiritual, que representa el esfuerzo que todo creyente debe realizar para ser mejor musulmán o mejor persona en general[8].

Tras este atentado comenzaron diversos ataques e invasiones, como la de Irak, en la que España participó en diversos aspectos. Más tarde se produjeron diferentes ataques por parte de distintas organizaciones como Al Qaeda o Estado Islámico, muchos de los cuales ya hemos mencionado anteriormente. Su finalidad es generar el miedo social y la retirada de tropas en las regiones, para poder establecer ellos un estado de terror y sometimiento a las leyes del Corán más radicalmente interpretadas.

Pero lo que no se sabe es que muchos, a su vez, han sido desmantelados gracias a fuertes redes de antiterrorismo, con agentes encubiertos tanto en físico como en la red. El ciberpatrullaje[9], eliminación de videos de radicalización, localización y detención de terroristas y diversas actividades más han supuesto, con el paso del tiempo, la asfixia de las células hasta el punto de forzar su desaparición. Los ejércitos pueden combatir en un frente físico, pero los agentes encubiertos de campo son vitales en la preparación y diseño de estos ataques. A su vez, los informáticos acaban con cuentas bancarias, recursos, contenidos dedicados a la radicalización entre otras acciones, acciones que por su contenido son confidenciales.

El terrorismo yihadista no ha acabado aun, a diferencia del etarra o el anarquista, pero las acciones de los distintos órganos gubernamentales e instituciones jurídicas están cercándolo a pasos agigantados.

Realizado un sucinto análisis del terrorismo desde una perspectiva histórica y social procedemos a estudiar, también someramente, su componente jurídico. Como punto de partida exponemos la definición de terrorismo dada por la Real Academia de la Lengua Española:

> *Delito que consiste en llevar a cabo delitos graves con la finalidad de subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo, alterar gravemente la paz pública, desestabilizar gravemente el*

---

8 DE LA CORTE IBAÑEZ, L.: "Breve guía sobre la amenaza yihadista", en *Athenea Paper*, vol. 2, núm. 2, 2007, pp. 42-45.

9 Es un término acuñado por el experto en ciberdelincuencia y fiscal español D. Javier Ignacio Zaragoza. Al referirnos al ciberpatrullaje nos referimos a la traslación del patrullaje policial clásico al mundo virtual.

funcionamiento de una organización internacional, o provocar un estado de terror en la población o en una parte de ella[10].

Así observamos que los terroristas tienen como objetivo la subversión del Estado o de su entramado socioeconómico con una motivación anterior que es la que informa su actuación. Este no es un aspecto menor puesto que la tenencia de una ideología que sustenta sus atrocidades es a su vez un estímulo para su realización. Sin embargo, en la mayor parte de las ocasiones, las ideas que sirven de base para estas actividades son también, como poco, no democráticas.

El objetivo puede ser muy distinto según el lugar o el momento en el que se lleve a cabo[11] mostrando así que las organizaciones no solo se limitan al ataque indiscriminado sino también a la defensa de sus miembros o de la ideología que les sirve de sustrato.

Como puede verse las motivaciones y los resultados de los atentados terroristas son de una envergadura colosal y suponen un verdadero quebradero de cabeza para los Cuerpos y Fuerzas de Seguridad del Estado quienes han tenido que estudiar a su enemigo para comprender y evitar su mal. En este ejercicio de comprensión y de investigación ha jugado un papel fundamental el protagonista de esta investigación, el agente encubierto, una figura relativamente reciente en los ordenamientos jurídicos, pero cuya labor ha sido muy importante para evitar la propagación de esta lacra.

Como conclusión y anticipo de lo que desarrollarán las páginas siguientes, el terrorismo ya no solo se desarrolla en escenarios concretos, sino que resulta ser un fenómeno con una fuerte nota de internacionalización y que ha desplegado también sus actividades en internet[12], lo que tiene un evidente correlato en la lucha por su erradicación.

---

10 Definición del delito de terrorismo por el *Diccionario panhispánico del español jurídico* (consultado el 18 de julio de 2021).

11 Por ejemplo: en el caso del asesinato del político español Miguel Ángel Blanco –que marcó un hito en la lucha antiterrorista en España- se buscaba presionar al Estado español para que acercara a los presos terroristas de ETA a los centros penitenciarios vascos o en el referencial atentado del 11-S perpetrado por Al-Qaeda fue ideado como un castigo a los EEUU por el apoyo de la potencia a los israelíes o su presencia en Arabia Saudí. Fundación Miguel Ángel Blanco https://www.fmiguelangelblanco.es/miguel-angel-blanco/su-vida/ (consultado el 18 de julio de 2021). En este sentido, véase también IGLESIAS VELASCO, A. J.: «La respuesta internacional ante los ataques terroristas contra Estados Unidos», en *Revista Electrónica de Estudios Internacionales,* núm. 4, 2002, pp. 1-2.

12 Al respecto, puede consultarse el Informe "El uso de internet con fines terroristas" elaborado por la Oficina de las Naciones Unidas contra la Droga y el Delito: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf (consultado el 28 de julio de 2021).

3. La figura del agente encubierto informático para la investigación del terrorismo

3.1 La necesidad de una regulación del agente encubierto para la lucha contra el terrorismo

Ya hemos podido observar de manera sucinta la historia de esta lacra a nivel mundial, así que es el momento óptimo de hablar de su antitético más importante en la actualidad, y herramienta fundamental para su erradicación: el agente encubierto.

El trabajo de esta figura es muy diferente al que se suele expresar en películas o literatura policiaca. A su vez, dependiendo del país, estamos ante diferentes sujetos con diversas capacidades, potestades y libertades. El trabajo y funciones de un agente encubierto americano serán muy diferentes a las de uno colombiano y, este, a su vez, poco se asemejará con su homólogo español. La diferencia es grande en cuanto al agente encubierto físico, el "tradicional"; sin embargo, en la nueva faceta, la del agente encubierto informático, sí que todos poseerán una serie de similitudes extrapolables al grueso de las naciones democráticas.

En España, pese a que ya existían de hecho con anterioridad, la Ley Orgánica 5/1999, de 13 de enero, introdujo una regulación jurídica sistemática y modificó la legislación procesal penal para incluir esta relevante figura[13]. Podemos atender a la interpretación del Tribunal Supremo español sobre la figura del agente encubierto en la STS 1140/2010, 29 de diciembre de 2010. En este caso solo hacía referencia al físico, es decir, a aquel cuya incursión se realiza en el mundo real y el cual tiene trato personal con el objetivo de la investigación. Cuando la ley se creó, esta hacía referencia a la lucha contra el crimen organizado, presuponemos que narcotráfico, trata de blancas o extorsiones. No por ello se excluían los casos de lucha antiterrorista, ya que el objeto de la sentencia citada anteriormente fue una investigación por delito de pertenencia a organización terrorista. Pocos años después, ocurrió la revolución de las redes: ordenadores, internet, webs, ocuparon nuestras vidas para quedarse. Y los sectores más peligrosos de la sociedad también los empezaron a usar, avalados por la privacidad y confidencialidad de sus acciones y la facilidad de intercambios monetarios en base a criptomonedas u otras divisas anónimas, que hace que a día de hoy, la mayor parte de la financiación de grupos terroristas recaiga en este tipo de finanzas tan

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

sumamente difíciles de investigar[14]. En este momento es cuando entran en juegos términos como Deep Web o Dark Web, que son las capas más profundas y más difíciles de acceder de internet, hasta el punto que, en algunas ocasiones, precisan de un navegador externo o una VPN propia[15]. La red es libre y ningún país posee un control sobre ella. Por ello, los delitos y su persecución son asumidos por los distintos países y organizaciones internacionales en función de su jurisdicción. Por ejemplo, si un hacker de sombrero negro (*hackers* relacionados con la ciberdelincuencia) realiza una estafa online desde Rumania, pero a páginas españolas, el delito que se le imputa será, en gran medida, tipificado en el Código Penal español, aunque no por ello el Gobierno rumano no colaboraría en su detención o tendría su propio derecho a enjuiciarle[16].

La pregunta que debemos hacernos en este punto es: ¿cómo se descubren estos delitos? La respuesta más breve es el ciberpatrullaje. En España los encargados de vigilar el espacio cibernético de manera habitual son los miembros de la Brigada Central de Investigación Tecnológica[17]. Revisan de manera exhaustiva cada página, cerrando y procesando aquellas que se vean involucradas en delitos de diversa índole, desde pornografía infantil, amenazas, fraudes online… En muchos casos, no es posible acceder a estas direcciones de manera anónima, sino que precisan de registro o de algún tipo de clave/identificador. Es necesario, de nuevo, realizar sus labores de manera encubierta. Nace ahora, de forma oficial, la figura del agente encubierto informático. Los agentes encubiertos no tienen que ser obligatoriamente de dicha Brigada, pero sí miembros de la Policía Judicial que actúen de manera voluntaria. Esta decisión es bastante controvertida en el caso del agente informático, puesto que en muchos casos sus labores se realizan en sede policial, y un civil o colaborador con conocimientos muchos más amplios podrían enfrentar mejor la tarea, siempre y cuando estuvieran en todo momento vigilados y controlados por un revisor.

---

14 YUSTE GONZÁLEZ, C.: "Deep web y monedas virtuales: entorno privilegiado para las organizaciones terroristas", en *Repositorio de Trabajos de Fin de Máster,* Universidad Internacional de La Rioja, 2015.

15 De facto, en la que se profesa la mayor cantidad de delitos es en la *dark web*, tal como señala LAVÍN PERRINO, I.: "Un paseo por la Deep Web", *en Repositorio de Trabajos de Fin de Máster*, Universitat Oberta de Catalunya, 2018.

16 ORTIZ PRADILLO, J. C.: "La investigación del delito en la era digital: los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación", en *Fundación Alternativas*, núm. 74, 2013.

17 Sobre las funciones, actuaciones y organización de este órgano policial, puede verse https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php# (consultado el 15 de julio de 2021).

Poseen, para su correcto desempeño, una serie de características muy específicas. Una de ellas consiste en que su activación sólo tiene lugar para actuaciones o investigaciones del Ministerio Fiscal, por lo que el cuerpo de policía pertinente no puede actuar en propia voluntad. Estos agentes también obran bajo una identidad supuesta, aunque no se les vea el rostro o interactúen físicamente con los delincuentes. El Juez de Instrucción es el único con capacidad para decidir si la operación se lleva a cabo, durante cuánto tiempo, y en qué términos. Esto sólo en el caso del AEI. Una vez esclarecidas las características con las que se activa una operación judicial con agente encubierto, veamos aquellas competencias que, en la mayoría de los casos, les son atribuidas. Un agente encubierto informático podría intercambiar archivos ilegales, analizarlos y, en el caso de encontrarse de manera presencial con el investigado, grabar las conversaciones, siendo esta última actuación regulada en el apartado 7 del art. 282 bis LECrim. Eso sí, es muy importante que todas estas acciones cuenten con un respaldo judicial y respeten los derechos fundamentales para no realizar ninguna acción no autorizada o inconstitucional que pudiese anular la prueba.

Las diferencias sobre el papel son claras, pero hoy en día gracias a la modernización general de ambos bandos, el trabajo de campo de un agente encubierto se ve muy dificultado sin apoyo informático y viceversa. La colaboración entre ramas y divisiones es, cada vez más, uno de los motivos por los cuales las investigaciones llegan a buen puerto y los implicados son procesados con todas las garantías y derechos constitucionales.

3.2 Diferencias entre el agente encubierto informático y el agente provocador

El agente encubierto informático a la hora de actuar debe respetar el ordenamiento jurídico. Así, para evitar posibles comportamientos ilícitos, resulta conveniente diferenciar entre esta figura y la del agente provocador.

A fin de analizar la actividad de un agente policial, hemos de tener en cuenta dos posibles conductas. La primera, sería aquella en la que el agente lleva a cabo una investigación con el objeto de reprimir o prevenir un delito planeado previamente por parte del presunto delincuente. En segundo lugar, cabe que el agente induzca al autor provocado a la comisión de un delito que no tenía previsto cometer. El primero de los supuestos sería lícito dentro de los límites del art. 126 de la Constitución Española, del art. 11 de la LO 2/1986 de Fuerzas y Cuerpos de Seguridad del Estado y de los arts. 282 y ss. de la Ley de Enjuiciamiento Criminal. Sin embargo, la segunda de las conductas constituiría un delito provocado.

El concepto doctrinal del agente provocador sería aquel que "provoca a otro a la comisión de un delito con el fin de que el autor provocado sea sancionado por el ilícito penal sin que tenga la voluntad de su consumación, poniendo en ello las medidas necesarias"[18]. Así, el agente provocador actúa con el fin de detener al delincuente en el instante, impidiendo la perfección del delito, mientras que el agente encubierto trata de conseguir información[19].

Para continuar examinando al agente provocador, cabe mencionar tres presupuestos que delimitan esta figura[20]:

1.º La provocación tiene por objeto la pena del autor provocado.

2.º El agente provocador no tiene la voluntad de la consumación del delito.

3.º La ausencia de dicha voluntad se refleja en la adopción de medidas que pretenden neutralizar la acción del autor provocado.

La "provocación al delito" se encuentra recogida en el artículo 282 bis LECrim en su apartado 5º) y se ha ido precisando a través de la numerosa jurisprudencia. En este sentido, podemos destacar la STS 395/2014, de 13 de mayo, la cual indica en su 4.º Fundamento de Derecho que el delito provocado se compone de tres elementos: a) un elemento subjetivo, constituido por la incitación engañosa a cometer un delito por parte del agente dirigida a quien no tiene intención de hacerlo; b) un elemento objetivo o teleológico, consistente en la detención del sujeto que comete el delito inducido; y c) un elemento material, que consiste en la inexistencia de riesgo alguno para el bien jurídico protegido y, como consecuencia, que conduce a afirmar la atipicidad de la conducta.

En un sentido similar se pronuncia el Tribunal Europeo de Derechos Humanos en las Sentencias de 1 de marzo de 2011 (caso *Lalas c. Lituania*) y de 5 de febrero de 2008 (caso *Ramanauskas c. Lituania*), expresando que "se considera que ha tenido lugar una incitación por parte de la policía cuando los agentes implicados (…) no se limitan a investigar actividades delictivas de una manera pasiva, sino que ejercen una influencia tal sobre el sujeto que le incitan a cometer un delito que, sin esa influencia, no se hubiera cometido, con el objeto de averiguar el delito, esto es, aportar pruebas y poder iniciar un proceso".

---

18 *Vid*. MUÑOZ SÁNCHEZ, J. *El Agente provocador.* Tirant lo Blanch, Valencia, 1995, p. 43.

19 ANAYA MARCOS, M. C.: "El agente encubierto" (Trabajo de Fin de Grado), Universidad de Salamanca, 2015, p. 28.

20 MOLINA PÉREZ, T.: "Técnicas especiales de investigación del delito: el agente provocador, el agente infiltrado y figuras afines", en *Anuario Jurídico y Económico Escurialense*, núm. 41, 2008.

Teniendo esto en cuenta, es posible afirmar que la causa del delito parte del comportamiento del agente provocador, delito que no llega a consumarse debido a la inmediata intervención de la policía. Es por ello que, dada su imposible perfección, así como por el principio de interdicción de la arbitrariedad de los poderes públicos (recogido en el art. 9.3 de la Constitución Española), el Tribunal Supremo español considera el delito provocado como penalmente irrelevante y procesalmente inexistente[21]. Asimismo, considera que "la punibilidad del delito provocado por las Fuerzas de Seguridad es incompatible con el Estado de Derecho"[22]. En consideración al art. 11.1 LOPJ, establece este mismo Tribunal que, otra de las consecuencias de la actuación del agente provocador, es que "la prueba del delito obtenida mediante la inducción al mismo es una prueba ilícita".

Por su parte, el Tribunal de Estrasburgo estableció en el precitado caso *Ramanauskas c. Lituania*, que "el interés público no podría justiciar la utilización de datos obtenidos tras una provocación policial", pues tal forma de operar es susceptible de privar al acusado de su derecho a un proceso equitativo[23].

En el caso español, la provocación al delito por parte de un agente policial se encuentra prohibida en el apartado 5 del art. 282 bis LECrim[24]. Es por ello que no es posible admitir la actuación del agente encubierto, puesto que de lo contrario se vulneraría el ordenamiento jurídico, quebrantando así el Estado de Derecho.

4. Las actuaciones del agente informático y su relevancia jurídico-procesal

4.1 Los riesgos constitucionales de las actuaciones del agente encubierto

Nuestra vida no puede entenderse sin la red, sin el mundo virtual, que tanta repercusión tiene a su vez en el que consideramos real. La evolución exponencial de la informática ha provocado que las instituciones en muchas ocasiones se queden obsoletas ante este fenómeno y su imparable y galopante

---

21 Ibid.

22 Sentencia del Tribunal Supremo de 20 de octubre de 1997.

23 MOLINA PÉREZ, T.: "Técnicas especiales…", *op. cit*.

24 El apartado 5 del art. 282 bis LECrim dispone que el agente encubierto estará exento de responsabilidad criminal por los actos que resulten necesariamente de la conducción de la investigación, siempre que guarden "la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito".

progreso[25]. Las instancias judiciales no han sido ajenas a esta obsolescencia. Sin embargo, la justicia está haciendo un notable esfuerzo por adaptarse a este nuevo mundo, intentando paliar el anacronismo del que adolecen algunas de sus prácticas.

El análisis de la potencial vulneración de derechos fundamentales se realizará, en gran medida, teniendo como base o referencia la normativa española, al considerarse esta pionera en el estudio de la figura[26] no solo a nivel europeo[27] sino también a nivel mundial[28]. La regulación de la institución es relativamente reciente, Ley Orgánica 13/2015 del 5 de octubre, que se incorpora a la Ley de Enjuiciamiento Criminal[29]. No obstante, su corta edad, no ha sido obstáculo para que hayan corrido ríos de tinta con diferentes mares como destino sobre su contenido.

Los derechos objeto de estudio serán la tutela judicial efectiva y la intimidad personal, el secreto de las comunicaciones y la limitación del uso de la informática[30], ya que resultan ser los más afectados por las actuaciones del agente encubierto informático.

Antes de proceder con el desarrollo conviene realizar una consideración: no debe olvidarse que la adjetivación de informático supone un cambio sustancial en la toma de decisiones, un tratamiento adaptado a su singularidad que difiere enormemente de lo realizado por su homólogo físico[31].

---

25 CARDOSO PEREIRA, F: *Agente encubierto y proceso penal garantista: límites y desafíos*, Tesis doctoral, Universidad de Salamanca, 2012, pp. 216-217

26 Dentro de la actuación del agente encubierto informático pueden diferenciarse dos tipos de actuaciones: el rastreo IP (Internet Protocol, por sus siglas en inglés) y el registro remoto sobre equipos informáticos. Ambas cuestiones ya han sido tratadas en epígrafes anteriores.

27 No obstante, en el ámbito continental, debe destacarse también la normativa alemana sobre la materia.

28 En este caso también puede mencionarse su homóloga estadounidense.

29 Siendo el objeto de estudio la normativa española debe mencionarse que los derechos que se expondrán serán los recogidos en la Constitución española de 1978 (en adelante, CE).

30 Los derechos citados se corresponden con los arts. 18.1, 18.2 y 18.4 y 24 CE.

31 BUENO DE MATA, F.: "El agente encubierto en internet: mentiras virtuales para alcanzar la justicia", en PÉREZ-CRUZ MARTÍN, A. J.; FERREIRO BAAMONDE, X. (coords.): "*Los retos del Poder Judicial ante la sociedad globalizada*. Publicaciones de la Universidade da Coruña, La Coruña, 2012, pp. 295-306, entiende que se trata de una figura que, si la trasladamos a internet, debe obligatoriamente "cambiar sus características y su *modus operandi* para adaptarlo a los entornos virtuales, pero sin hacer que pierda su esencia. Una esencia polémica y muy debatida basada en el engaño y con la que se trataría de utilizar técnicas usadas para delinquir como técnicas a su vez de investigación o combate de este tipo de delincuencia".

La LECrim establece lo necesario de la autorización judicial para el comienzo de las actuaciones con el conocimiento de las mismas de la fiscalía[32], muestra así el legislador la importancia que le otorga a estas actuaciones. Además, el auto judicial deberá estar informado por los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad[33]. De entre estos, el de proporcionalidad actúa como un *primus inter partes*.

Su estudio se fundamenta en la justicia, la dignidad de la persona y de la privación de la arbitrariedad de los poderes públicos. Nos encontramos ante un principio constitucional al que hay que acogerse cuando se lleven a cabo medidas que restrinjan algún derecho fundamental.

El art. 588 bis a 5 LECrim, lo recoge dentro de sus principios rectores y, en lo referente al agente encubierto, el art. 282 bis LECrim establece que este último deberá actuar y mantener la proporcionalidad de acuerdo con los fines previstos en la investigación.

De manera que, el principio de proporcionalidad constituye el límite más estricto de los derechos fundamentales asegurando su vigencia en el desarrollo del proceso.

Sin embargo, la proporcionalidad por sí sola no es suficiente para proteger eficazmente los derechos fundamentales y precisa de la ponderación para lograr su completa protección. A lo anterior se suman una serie de valores, antes citados, cuya exposición se hace necesaria en tanto actúan como informadores de la actuación judicial convirtiéndose en contrapesos del *ius puniendi* del Estado[34].

La especialidad de la actuación, en otras palabras, la existencia de indicios suficientes de que la organización objeto de investigación está cometiendo alguno de los delitos tipificados en el art. 282 bis de la LECrim. Tiene que existir un hecho delictivo en avanzada fase de desarrollo. No es suficiente con la mera sospecha, sino que tiene que haber hechos objetivamente determinantes, es decir, tiene que ser más que posible que los individuos estén llevando a cabo conductas delictivas[35]. La Policía Judicial es la encargada de recopilar los indicios necesarios para entregarlos al Juez junto a la solicitud de la investigación informática. Es necesario que la actuación se lleve a cabo respetando un mínimo de garantías y que el medio resulte útil en la investigación. Igualmente,

---

32 Véase el art. 588 bis a LECrim.

33 Ídem.

34 Al respecto, resulta de interés BACHMAIER WINTER, L. (coord.): *Terrorismo, proceso penal y derechos fundamentales*. Marcial Pons, Madrid, 2012.

35 Sentencia del Tribunal Supremo 513/2010, de 2 de junio.

es imprescindible que el juez en la toma de decisiones atienda a los informes policiales[36].

La idoneidad, es decir, que sea apropiada para conseguir datos útiles para la investigación de la delincuencia organizada. Esta idea se apoya en el Auto TS de 18 de junio de 1992 que indica que "*resulta indispensable que existan indicios, lo que no puede equivaler jamás a sospechas o conjeturas*" (Sentencias del Tribunal Constitucional 174/1985 y 175/1985, ambas de 17 de diciembre). Es necesario que alcance el fin constitucionalmente legítimo perseguido con ella, así está establecido en el art. 8 del Convenio Europeo de Derechos Humanos, que prohíbe cualquier injerencia de la autoridad pública en el ejercicio de este derecho "*sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*"[37].

La necesidad o subsidiariedad de la medida: para que el Juez de su autorización es imprescindible que no exista otra medida menos perjudicial e intrusiva para los derechos fundamentales, así se establece en el artículo 282 bis LECrim "su necesidad a los fines de la investigación". La infiltración tiene que ser la única opción para la obtención de indicios relevantes relacionados con la investigación terrorista.

La proporcionalidad al utilizar la figura únicamente en aquellos casos que así lo requieran por su repercusión o por su gravedad. El sacrificio de derechos que hace el Estado es muy alto, por lo tanto, el delito tiene que tener cierta enjundia. Una valoración realizada por el juzgador y que se recoge en el auto que permitirá o denegará la infiltración.

La motivación, en el auto, el juez tiene que motivar de manera explícita y detallada todos los requisitos mencionados anteriormente, tal y como se recoge en el artículo 282 bis LECrim al establecer que tiene que ser una "*resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación*", además de constar la afectación de los derechos fundamentales del investigado. Asimismo, debe exponer de manera prolija las circunstancias que rodean al caso concreto y motivar la autorización atendiendo a los principios vistos con anterioridad y al encaje de la actividad delictiva en el tipo pertinente[38].

---

36 GARCÍA LÓPEZ, E., "Agente encubierto y agente provocador: ¿dos figuras incompatibles?", en *Diario La Ley*, núm. 5822, 11 de julio de 2003, pp. 1504-1506.

37 Ibid.

38 DEL POZO PÉREZ, Marta, "El agente encubierto como medio de investigación de la delincuencia organizada en la ley de enjuiciamiento criminal español", en *Criterio Jurídico*, vol. 6, 2006, pp. 267-310.

Una vez vistos los principios que informan toda la actuación judicial durante el proceso que nos ocupa podemos abordar las posibles injerencias en los derechos fundamentales del investigado o en los de las víctimas del presunto delito.

En el caso de la vulneración del derecho a la tutela judicial efectiva, esta puede ocurrir por la falta de conocimientos sobre la realidad informática del juez. Como se ha visto anteriormente, la labor del agente comienza con la resolución judicial motivada y que pormenoriza cuestiones como el ámbito temporal y el de actuación de la labor de este funcionario –dentro de unos límites prefijados-. Así, se deposita en el juez un amplio margen de actuación para determinar las directrices y límites del agente en su investigación, una amplitud quizás planteada por el legislador para evitar la temida obsolescencia de la norma, evitando así la inclusión de preceptos prolijos que puedan tornarse ineficaces en un corto periodo de tiempo. Ahora bien, los jueces no tienen por qué conocer los últimos avances informáticos ni tan siquiera los rudimentos de la ciencia informática[39].

Derivado de lo anterior, pueden darse casos en los que, por la ignorancia del juez, aunque pueda recibir asistencia por profesionales, se produzca un perjuicio para la presunta víctima que puede ver minoradas las posibilidades de captura del presunto criminal. Una cuestión que se complica en el terrorismo al contar habitualmente las organizaciones con unos equipos tanto técnicos como humanos de alta calidad[40].

Las anteriores consideraciones se han realizado respecto de la víctima, pero también merece destacarse otra posibilidad respecto al presunto culpable y es que el conjunto de los ciudadanos tenemos derecho[41] a la tenencia de un

---

39 CARDOSO PEREIRA, F.: *Agente encubierto y proceso penal garantista: límites y desafíos*. Tesis doctoral, Universidad de Salamanca, 2012. Texto disponible en abierto en (https://gredos.usal.es/jspui/bitstream/10366/121134/1/DDAFP_CardosoFlavio_Tesis.pdf) (consultado el 18 de julio de 2021).

40 ZAFRA ESPINOSA DE LOS MONTEROS, M. R.: "Las reglas de exclusión probatoria al hilo del desarrollo de la infiltración policial", en *Temas Socio-Jurídicos*, vol. 57, núm. 57, pp. 71-101, entiende que "esta sofisticación y profesionalización supone la proclamación como expertos en técnicas delictuales (como la supresión de la prueba), en técnicas jurídicas o económicas (que le permiten eludir la acción de la justicia), médicas o informáticas" (pp. 72-73).

41 Un derecho recogido en la Declaración Universal de Derechos Humanos, adoptada y proclamada por las Naciones Unidas, en su art. 10: "Toda persona tiene derecho, en condiciones de plena igualdad, a ser oída públicamente y con justicia por un tribunal independiente e imparcial, para la determinación de sus derechos y obligaciones o para el examen de cualquier acusación contra ella en materia penal". Además, se concreta de similar manera en numerosos textos constitucionales como el español (art. 24.2 CE) o el colombiano (art. 29).

proceso con todas las garantías[42]. Estas garantías juegan un papel fundamental en el material probatorio, en otras palabras, en las pruebas. La cadena de custodia tiene por objeto evitar las interferencias o variaciones en las pruebas desde que son conseguidas hasta que se muestran o utilizan en el juicio[43]. La búsqueda de la idéntica identidad opta por diferentes procedimientos según nos encontremos ante un agente de tipo físico que uno encubierto, no suponiendo en ningún caso un perjuicio para quien busca de los tribunales la mayor de las efectividades[44]. En aquellos casos en los que alguno de los eslabones falle, el presunto culpable encontrará minorado su derecho[45]. Puede añadirse que, en el caso de las pruebas de tipo informático, en pro de quien tiene que ajustarse a ellas, estas se deberían acompañar de un informe[46] en el que se detallen las características de las mismas y se expliquen aquellos conceptos y expresiones eminentemente digitales que puedan presentar dificultades para aquellos legos en la materia, garantizando así que la incomprensión no suponga un riesgo para el correcto desarrollo del proceso.

El derecho a la intimidad está íntimamente relacionado con la identidad. Es aquí donde surge un interrogante al plantearnos en qué medida la persona se reconoce en la Red cuando utiliza un apodo o una identidad falsa, como en el caso del agente encubierto.

En la Red la identidad del mundo físico sufre una reinterpretación y pasa a identificarse con un binomio formado por la persona detrás de este apodo y del dispositivo que utiliza para navegar. Por ello, la importancia del rastreo de la IP[47].

---

42 CALDERÓN CUADRADO, M. P.: "El derecho a un proceso con todas las garantías (aspectos controvertidos y jurisprudencia del Tribunal Constitucional)", en *Cuadernos de Derecho Público*, núm. 10 (mayo-agosto, 2000), esp. pp. 155-160.

43 CÁNOVAS RODRÍGUEZ, A*: Agente encubierto online* (Trabajo de Fin de Grado). Universitat Autònoma de Barcelona, 2017.

44 DEL POZO PÉREZ, M. "La cadena de custodia: tratamiento jurisprudencial", en Revista General de Derecho Procesal, núm. 30, 2013.

45 FIGUEROA NAVARRO, C.: "La regulación de la cadena de custodia en España: previsiones legales y desarrollos jurisprudenciales sobre la cadena de custodia de la fuente de prueba", en FIGUEROA NAVARRO, C. (coord.): *La cadena de custodia en el proceso penal*. Edisofer, Madrid, 2015.

46 AURELIO GARCÍA, J.: "La cadena de custodia aplicada a la informática", en *El Blog del Perito Informático*, 2013. Disponible en http://www.informaticoforense.eu/la-cadena-de-custodia-aplicada-a-la-informatica-i/ (consultado el 18 de julio de 2021).

47 Para conocer la IP de un dispositivo se precisa de la colaboración de los proveedores de servicios informáticos, previa resolución judicial habilitante. Art. 588 ter (j) LECrim.

En este caso, así como en el que le ha precedido, como en el que le sucederá, el interés público prevalece sobre el particular. Más si cabe en casos en los que puede estar en juego la subversión del Estado. Esto no supone la dación de una patente de corso para el agente, puesto que la restricción de los derechos fundamentales debe siempre realizarse a través de una regulación estricta y garantista que tenga siempre en cuenta la presunción de inocencia, intensificada en un Estado de Derecho[48].

El secreto de las comunicaciones solo puede realizarse mediante resolución judicial[49]. Ahora bien, la revelación del contenido de los intercambios de información no conlleva su conversión en pública ni tampoco su difusión más allá de las necesidades judiciales, en este sentido, el art. 588 bis (d) LECrim recoge la posibilidad de que se sustancien en piezas separadas.

La interceptación de las comunicaciones puede conllevar que el agente tenga conocimiento, a través de las mismas, de otras informaciones relevantes no solo del propio investigado sino de terceros, quienes verían afectados sus derechos sin ningún tipo de motivación[50]. Un problema de difícil subsanación y que supone la existencia de un mínimo gravamen de compleja reparación.

Finalmente, conviene apuntar que la maléfica utilización de la Red para la comisión de delitos se complementa, paradójicamente, con el benéfico uso que pueden llevar a cabo las Fuerzas y Cuerpos de Seguridad del Estado de los recursos que la misma les brinda para evitar su comisión o impedir su impunidad según el caso.

---

48 DEL POZO PÉREZ, M.: "El agente encubierto como medio de investigación de la delincuencia organizada en la Ley de Enjuiciamiento Criminal española", en *Criterio Jurídico,* núm. 6, 2006, pp. 295-296.

49 Pues se trata de un derecho fundamental (art. 18.3 CE) con el máximo nivel de protección jurisdiccional.

50 En este caso, como posible respuesta al interrogante, puede citarse lo referido a descubrimiento o tenencia de información adyacente obtenida en el transcurso de la investigación la jurisprudencia española sigue la teoría del descubrimiento inevitable la cual permite que en aquellos casos en los que la prueba en cuestión fuera a ser descubierta inevitablemente sin necesidad del material probatorio ilícito que permitió su origen. Así lo explica la Sentencia del Tribunal Supremo 885/200, de 21 de mayo: "[C]uando la experiencia indica que las circunstancias hubieran llevado necesariamente al mismo resultado, no es posible vincular causalmente la segunda prueba a la anterior, pues en tales casos faltará la llamada, en la terminología del Tribunal Constitucional, «conexión de antijuridicidad», que, en realidad presupone, en todos los casos, una conexión causal".

4.2 La entrada al proceso de las pruebas obtenidas por el agente encubierto informático

a) La necesaria autorización judicial

Para iniciar la intervención del agente encubierto informático, el Juez de Instrucción deberá dictar un auto judicial, concediendo la autorización para que el agente encubierto lleve a cabo la investigación correspondiente en un canal de comunicación cerrado de acuerdo con el apartado 1 del artículo 282 bis LECrim[51]. Dada la potencialidad lesiva de sus actuaciones respecto de los derechos fundamentales, en ningún caso podrá acordar el Ministerio Fiscal tal autorización. Por su parte, el Ministerio del Interior habrá de facilitar la identidad supuesta y los documentos necesarios para el desarrollo ordinario de las actividades correspondientes[52].

En el auto dictado por el Juez de instrucción, se recogerán las medidas o directrices bajo las cuales el agente encubierto informático estará obligado a cumplir su cometido. En cualquier caso, la autorización judicial tiene una doble finalidad: por un lado, resulta necesaria para llevar a cabo la infiltración en sí misma, y, por otro, sirve como marco establecido por el Juez para intercambiar o enviar archivos ilícitos por razón de su contenido. En la práctica, esto sirve para poder acceder a lugares donde captar nuevos miembros para sus organizaciones terroristas y para que se permita la entrada y obtener la clave para ser uno de ellos.

Se tienen que dar unas características determinadas para que el agente pueda obtener la autorización para la infiltración; muy especialmente, una formación altamente especializada en conocimientos informáticos y psicológicos. Debe tenerse en cuenta que el agente encubierto informático, como otros funcionarios que desempeñan investigaciones tecnológicas, están expuestos a un contenido impactante y extremo que puede producir consecuencias psicológicas, por lo que el Juez no podrá en ningún caso obligar a un determinado componente de la Policía Judicial para ejercer como agente encubierto informático[53].

---

51 Como señala el referido artículo, la resolución por la que se acuerde la intervención del agente "deberá consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto. La resolución será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad".

52 El artículo 282 bis LECrim establece que "la identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico y social bajo tal identidad".

53 DEL POZO PÉREZ, M.: "El agente encubierto…", *op. cit.*

b) La supervisión de las actuaciones del agente

Es evidente que este tipo de agentes está expuesto a situaciones muy extremas que pueden llegar incluso a que se convierta en un miembro más de la organización, olvidando su verdadera finalidad: a medida que avanza en la investigación, existe un mayor grado de implicación con la organización por parte del agente. Crecen las expectativas de obtener datos útiles, pero también aumenta el riesgo para el Estado de Derecho de que el funcionario cometa actos susceptibles de ser constitutivos de delito.

Por ello, el agente encubierto reportará lo que vaya descubriendo en el menor tiempo posible al órgano jurisdiccional autorizante. Para hacerlo con garantías de que la investigación se desarrollará de forma eficaz y garantista, existe en la práctica operativa la figura del supervisor: un mando policial que conoce al agente y puede controlar sus señales de alarma[54]. Al mismo tiempo, el agente va a informar de sus actividades y descubrimientos a su supervisor y, a fin de proteger su identidad, será este último quien informe al juez de forma constante y fehaciente.

La decisión de infiltrar a un funcionario de policía en un específico grupo organizado que se esté investigando debe partir de un mando policial. La iniciativa, por tanto, es algo que compete exclusivamente a las Fuerzas y Cuerpos de Seguridad del Estado, ya que son los más indicados para determinar y valorar las dificultades que puedan derivar de la infiltración y los posibles frutos que puedan derivarse de ella. Además, deben ser capaces de garantizar la vida y la seguridad del funcionario que voluntariamente se infiltra.[55]

En la práctica, como ya hemos mencionado, para las actuaciones de este agente encubierto habrá que utilizar al supervisor, que es la figura intermediaria para mantener el contacto entre el órgano jurisdiccional y el agente encubierto. El agente encubierto tendrá que comunicarle la información al supervisor y pedirle las autorizaciones que necesite para llevar a cabo actuaciones que sean restrictivas de derechos fundamentales. Sobre esto, la legislación procesal dispone la necesidad de que el Juez esté permanentemente informado, pero nada obliga a que deba hacerlo personalmente el infiltrado. El Juez, por tanto,

---

54 SANCHO MONCLÚS, M.: "La figura del agente encubierto en el Derecho procesal penal español", Trabajo de Fin de Grado, Universidad de Zaragoza, p. 20.

55 MONTÓN GARCÍA, M. L.: "Técnicas penales de investigación: confidente,agente provocador, agente encubierto ("físico") y agente encubierto informático", en DÍEZ-PICAZO GIMÉNEZ, I.; VEGAS TORRES, J. (coords.): *Derecho, Justicia, Universidad. Liber amicorum de Andrés de la Oliva Santos*, vol.II. Centro de Estudios Ramón Areces, Madrid, 2016, pp. 2135-2152.

recabará toda la información del supervisor, lo que convierte a esta figura en un elemento clave en este tipo de operaciones.

En suma, el supervisor es el responsable directo del agente encubierto informático y debe realizar una función de vigilancia respecto de las actividades realizadas por él, así como de interlocución con el resto de los investigadores[56]. Además, coordinará el dispositivo de seguridad, transmitirá al agente todo aquello que sea necesario y recogerá de este la información y las fuentes de prueba obtenidas para ponerlas en conocimiento del instructor que autorizó la operación. Finalmente, tendrá que interpretar las alertas sobre el peligro que el encubierto esté sufriendo en cada momento concreto, convirtiéndose a un mismo tiempo en su jefe, su enlace y su protector. Asimismo, algo que es muy importante, es que será quien detecte las posibles señales de alarma en su actuación o comportamiento que puedan llevarle a pensar que el funcionario de policía se integre voluntariamente en la organización criminal y pierda su compromiso policial, o bien, que la situación de infiltrado le está afectando más allá de lo razonable física y psicológicamente, lo cual, si sucede, llevaría a poner fin a la medida. Por ello, el controlador o supervisor debe ser el primer eslabón para evaluar y fiscalizar su actuación.

Estas conductas del agente encubierto, en relación con la responsabilidad penal, deberán valorarse teniendo en cuenta circunstancias que tuvieran lugar en el momento de comisión del presunto hecho delictivo, considerando que, para ello, además de atender al testimonio del agente encubierto, también tendremos que acudir a los datos relativos a la investigación; datos que, por descontado, el agente tiene la obligación de comunicar con la mayor rapidez posible al supervisor.

c) Consecuencias probatorias de los descubrimientos efectuados por el agente

El elemento más importante que debe tenerse en cuenta a la hora de estimar el valor probatorio de los hallazgos efectuados es el testimonio del propio agente encubierto informático[57]. El punto de partida debe ser el artículo 717 LECrim, según el cual, las declaraciones de las autoridades y funcionarios de la Policía Judicial "tendrán el valor de declaraciones testificales, apreciables como estas según las reglas del criterio racional".

---

56 CLUSA LÓPEZ, A.: "El agente encubierto informático" (Trabajo de Fin de Grado). Universidad de Zaragoza, 2019.

57 Ibid.

Uno de los problemas que nos podemos plantear viene determinado por los casos en que el agente encubierto informático, dentro de sus funciones, sea testigo de una confesión por parte del sujeto investigado. Existe en este supuesto un confrontamiento entre el artículo antes mencionado y la jurisprudencia de los últimos años que entiende que, de acuerdo con el principio acusatorio, la confesión efectuada por el investigado ante el agente no puede ser valorada por los tribunales a la hora de dictar sentencia.

Esto está plasmado en el Acuerdo del Pleno No Jurisdiccional de la Sala Segunda del Tribunal Supremo de 3 de junio de 2015, donde se señala que "Las declaraciones ante los funcionarios policiales no tienen valor probatorio", es decir, que no pueden operar como corroboración de los medios de prueba y tampoco "cabe su utilización como prueba preconstituida en los términos del artículo 730 de la LECrim". Tampoco pueden ser incorporadas al acervo probatorio mediante la llamada como testigos de los agentes policiales que las recogieron[58].

Sin embargo, cuando los datos objetivos contenidos en la autoinculpación son acreditados como veraces por verdaderos medios de prueba, el conocimiento de aquellos datos por el declarante, evidenciado en la autoinculpación, puede constituir un hecho base y válido para efectuar inferencias lógicas. A estos efectos, para que sea posible dejar constancia de la validez y el contenido de la declaración policial, los agentes que la presenciaron, aunque sea en el espacio virtual, deberán prestar testimonio en el acto de juicio oral.

La mayor vulneración de considerar que el agente es testigo de una posible confesión del investigado en relación con una actividad terrorista es la vulneración del derecho a no declarar contra sí mismo, recogido en el artículo 24 de la Constitución. Por tanto, habría que valorar también si existen otros indicios que puedan ser tomados en consideración como prueba de cargo y que no estén vulnerando este u otros derechos fundamentales a fin de constatar su uso de forma legítima.

La consecuencia que tiene que una prueba vulnere derechos fundamentales, que se haya obtenido sin la correspondiente autorización judicial o que el agente encubierto no haya respetado los parámetros prefijados por el Juez, deberá ser la ilicitud radical de la prueba y, por tanto, la imposibilidad de usar su contenido en el acto del juicio oral. Hay que destacar también que,

58 En la doctrina, entre otros muchos, véanse especialmente ASENCIO MELLADO, J. M.: *Prueba prohibida y prueba preconstituida*. Trivium, Madrid, 1989; ARMENTA DEU, T.: *La prueba ilícita: un estudio comparado*. Marcial Pons, Madrid, 2011.

si una prueba es considerada nula, todas las demás pruebas que deriven de ella también habrán de entenderse como tal[59].

4.3 Colaboración internacional

Como ya hemos tenido ocasión de apuntar, la liberalización del comercio y el notable desarrollo que han tenido las comunicaciones han contribuido irremediablemente a la expansión de las actividades de las bandas organizadas más allá de la escala local o regional. Además, asistimos a un contexto en que las fronteras tienden a desdibujarse para potenciar la libre circulación de personas, servicios y bienes, como en el caso de la Unión Europea. Ambos factores, junto a muchos otros, posibilitan que los grupos de delincuencia organizada se instalen en varios Estados o en aquellos donde la labor de investigación policial sea menos intensa e, incluso, que puedan colaborar entre ellos, por lo que existen mayores dificultades a la hora de controlarlos.

En nuestra opinión, el agente encubierto, unido al establecimiento de cauces más eficientes para la cooperación procesal internacional, se instituye como un mecanismo extraordinariamente útil para luchar contra un terrorismo que ya no puede combatirse con los medios tradicionales.

Conviene en este momento referirse sucintamente a alguno de los instrumentos de cooperación internacional en el ámbito de la ciberdelincuencia[60], ya que las organizaciones supraestatales han desarrollado mecanismos para combatir el terrorismo.

En primer lugar, debemos destacar la importancia en el ámbito de la Unión Europea de EUROJUST[61]. Se trata de un órgano cuya labor consiste en el refuerzo de la cooperación judicial entre los Estados que forman parte de la

---

59 Se trata de la célebre doctrina de los frutos del árbol envenenado. Sobre sus orígenes y consecuencias prácticas, vid. MIRANDA ESTRAMPES, M.: *Prueba ilícita y regla de exclusión en el sistema estadounidense: crónica de una muerte anunciada*. Marcial Pons, Madrid, 2019.

60 El Convenio sobre Delincuencia, hecho en Budapest el 23 de noviembre de 2001, establece el marco y los principios generales para la cooperación procesal internacional y la asistencia judicial mutua, de forma que los Estados puedan cooperar entre sí en la mayor medida posible en materia penal para lograr investigaciones eficaces, especialmente en "los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos".

61 Se trata de la Unidad de Cooperación Judicial de la Unión Europea, un órgano creado en el año 2002 para mejorar la coordinación de las investigaciones y el ejercicio de las acciones penales, además de la cooperación entre los Estados miembros en el ámbito de la delincuencia transfronteriza.

Unión Europea a partir de la adopción de medidas estructurales que permitan una mayor coordinación de las investigaciones y actuaciones judiciales que tengan relevancia más allá del territorio de un Estado.

A partir del reconocimiento de la asistencia judicial mutua, es posible establecer medidas cautelares, donde se incluyen, entre otras, la conservación inmediata de datos informáticos o el acceso transfronterizo a los datos virtuales almacenados[62]. La Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, establece un régimen único para la obtención de pruebas en los casos transfronterizos, basándose en el principio de reconocimiento mutuo y rigiéndose por el ordenamiento jurídico del Estado de ejecución, de manera que una resolución emitida por una autoridad judicial de un Estado miembro sea reconocida y pueda ser ejecutada en otro Estado miembro de la Unión.

Además, se han creado órganos para luchar de la manera más eficaz posible contra el fenómeno de la ciberdelincuencia[63]. Además de EUROJUST, destaca la importancia del Centro Europeo de Ciberdelincuencia de EUROPOL. Su misión principal es desarticular las operaciones de bandas organizadas que cometen delitos, especialmente en el ámbito informático, apoyando y coordinando investigaciones llevadas a cabo por los Estados miembros. También en el ámbito europeo nos encontramos con ENISA, la Agencia Europea para la Red y la Seguridad de la Información, donde se encuentran los mayores expertos de ciberseguridad de Europa.

Debemos indicar que, en el ámbito de los países del Caribe, opera la Unión Internacional de Telecomunicaciones (ITU), un organismo de las Naciones Unidas especializado en tecnologías de la información y comunicación, y que dicho organismo, en estrecha colaboración con la Comunidad del Caribe (CARICOM), ha elaborado un Código Modelo legislativo en materia de ciberdelitos. En dicho texto, se apuesta por la previsión normativa de que únicamente para los delitos considerados graves, las autoridades puedan utilizar instrumentos de investigación como *keyloggers* o *remote forensic software* para averiguar las contraseñas utilizadas por la persona investigada[64].

---

62 QUEVEDO GONZÁLEZ, J.: *Investigación y prueba del ciberdelito.* Sepín. Madrid, 2017. Téngase en cuenta que, en el ámbito español, únicamente el artículo 276 de la Ley Orgánica del Poder Judicial hace mención a las peticiones de cooperación internacional, remitiéndose por lo demás a las distintas normas internacionales.

63 Ibid.

64 ORTIZ PRADILLO, J. C.: "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", en PÉREZ GIL, J. (coord.): *El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar y probar el delito*. La Ley, Madrid, 2012, pp. 267-310.

5. Conclusiones

Al inicio de esta ponencia expusimos la magnitud del terrorismo a nivel internacional en la sociedad y la necesidad de la utilización de instrumentos por parte de los Estados para hacer frente a este creciente fenómeno. Como observamos, la complejidad de la realidad tecnológica y delictiva en un mundo globalizado e interconectado requiere que estos instrumentos sean técnicamente avanzados, siendo el agente encubierto informático una de esas herramientas que ha demostrado ser capaz de neutralizar la acción de las organizaciones terroristas a través de la incursión por parte de un miembro de las Fuerzas y Cuerpos de Seguridad del Estado en estas estructuras delictivas. La actuación del agente en este supuesto se justifica en el derecho a la seguridad de la ciudadanía y en la evitación de la ruptura de la estabilidad social dado que el terrorismo, entre otras consecuencias, podría alterar la paz pública, así como suprimir el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales de un Estado. Sin embargo, esta actividad ha de ser desarrollada con suma cautela pues, de lo contrario, se podrían ver afectados los derechos fundamentales de aquellas personas que están siendo investigadas, así como de aquellas que sean condenadas, quedando así prohibidas, entre otras actuaciones, la figura del agente provocador o la infracción del principio de proporcionalidad.

De este modo, la aparición del terrorismo pone de manifiesto un consabido debate entre la seguridad y el respeto de las libertades y de los derechos fundamentales. Así, a mayor seguridad, mayor restricción de derechos y, a menor seguridad, menor restricción de derechos. Ahora bien, resulta necesario lograr una armonía entre estos bienes jurídicos. De tal manera que, junto a la búsqueda de una respuesta eficaz frente al terrorismo a través del uso de la tecnología, debemos asegurar el respeto de los derechos fundamentales y el cumplimiento de la ley, no pudiendo justificar el empleo de cualquier método de investigación y prevención del delito, sino únicamente de aquel mecanismo que se sostenga en una base legal que regule sus requisitos, sus garantías y sus límites. En otras palabras, con el objeto de evitar la práctica del denominado "Derecho procesal y penal del enemigo" que se basa en la necesidad de proteger la sociedad contra determinados peligros, se ha de rehusar el empleo de medidas que no respeten los límites propios de un Estado de Derecho.

Como hemos podido analizar, para dar una respuesta al terrorismo es necesario aplicar el Derecho penal y el Derecho procesal, resultando imprescindible un proceso penal con todas las garantías que permita aplicar la ley penal e investigar las conductas delictivas. Así, a fin de evitar una respuesta propia del "Derecho del enemigo" por ser considerada excesiva, se deben tener

en cuenta tres principios básicos a la hora de hacer frente a la criminalidad terrorista: la proporcionalidad; la necesidad; y la idoneidad.

Una vez examinada la figura del agente encubierto informático y la criminalidad organizada, consideramos que es necesaria una solución tanto nacional como internacional para afrontar el terrorismo manifestado en estos dos niveles, terrorismo que a partir de los atendados del 11 de septiembre deja de ser un fenómeno interno para pasar a convertirse en un fenómeno global. En esta tarea, los diferentes Estados, aunque legislen de forma distinta, no han de olvidar los valores éticos que prevalecen frente a los avances tecnológicos empleados para afrontar esta realidad delictiva. En este sentido, cabe recordar el vigente Estado Social y Democrático de Derecho, resultante de dos siglos de transformación desde la revolución francesa y que exige el respeto de los derechos de los ciudadanos y de los valores superiores del ordenamiento jurídico, que son el fundamento del orden político y de la paz social.

En nuestra opinión, el agente encubierto informático resulta ser una técnica que ostenta un papel relevante en el panorama del terrorismo actual dado que ha conseguido resultados eficaces en la desarticulación de estas organizaciones criminales. No obstante, deben importarse elementos éticos para el uso de esta figura, pues la seguridad nacional e internacional no pueden justificar una utilización indiscriminada de los medios tecnológicos que resulte contraria a los derechos y a las libertades fundamentales.