Cuadernos de RES PUBLICA en derecho y criminología
Nº En prensa ISSN: 2990-0697 DOI: 10.46661/respublica.12120.

Agente encubierto informático. Informe de derecho comparado

Computer undercover agent. Comparative law report

Andrés Soriano Guillamón
UCAM. Universidad Católica San Antonio de Murcia
andresorg@hotmail.com
ORCID: 0009-0005-8914-1487

César Augusto Giner Alegría
UCAM. Universidad Católica San Antonio de Murcia
caginer@ucam.edu
ORCID: 0000-0002-9743-7414

Resumen

Derivado de la Globalización Virtual y los avances de las nuevas Tecnologías de la Información y Comunicaciones, Internet se ha erigido como una herramienta imprescindible en nuestra vida cotidiana, implementando nuevas formas de comunicación, trabajo y ocio. Pero a pesar de toda esta modernidad, en la sociedad han emergido conceptos como el phishing, malware, ramsonware, cryptojacking; que, sumados a otros de mayor connotación subversiva como ciberguerra, amenazas híbridas, etc., han condicionado a la Comunidad Internacional al favorecimiento de una resiliencia común, como forma unísona de combate frente a la ciberdelincuencia. Para ello se fraguó por el Consejo de Europa, el Tratado de derecho internacional público y privado, con el que todos los países adheridos se comprometen a reconfigurar su ordenamiento jurídico y procesal, favoreciendo la implementación de nuevas formas de investigación con las que poder hacer frente a las contemporáneas redes de criminalidad organizada, caracterizadas por su descentralización y transnacionalidad, emergiendo con ello una reciente figura procesal de investigación policial, el Agente Encubierto Informático.

Palabras clave: Agente Encubierto informático, ciberdelincuencia, ciber investigación.

Abstract

Derived from Virtual Globalization and the advances of the new Information and Communication Technologies, the Internet has emerged as an essential tool in our daily lives, implementing new forms of communication, work and leisure. But, despite all this modernity, concepts such as phishing, malware, ransomware, cryptojacking have emerged in society; which, added to others of a more subversive connotation such as cyberwar, hybrid threats, etc., have conditioned the International Community to favor a common resilience, as a unison way of combating cybercrime. For this, the Council of Europe forged, the Convention on Cybercrime. Public and private international law treaty, with which all member countries undertake to reconfigure their legal and procedural system, favoring the implementation of new forms of investigation with which to deal with contemporary organized crime networks, characterized by their decentralization and transnationality, thus emerging a recent procedural figure of police investigation, the Computer Undercover Agent.

Keywords: Computer Undercover Agent, cybercrime, cyber investigation.

Cómo citar este trabajo: Soriano Guillamón, Andrés y Giner Alegría, César Augusto. (2025). Agente encubierto informático.Informe de derecho comparado. *Cuadernos de RES PUBLICA en derecho y criminología,, 01–21. https://doi.org/10.46661/respublica.12120.*

Recepción: 30.05.2024 **Aceptación:** 08.07.2025 **Publicación:** en prensa

1. Introducción

Según Manuel Castells (2006), acerca de la "sociedad red", la cual definió como "el paradigma tecnológico de nuestro tiempo, un naciente universo digital que se encuentra en permanente transformación y que se retroalimenta, a la vez que incide directa o indirectamente, en la vida de millones de personas", quiere decir que la irrupción de las nuevas tecnologías en nuestros tiempos está generando un mundo nuevo lleno de oportunidades, donde paralelamente crece la delincuencia, y eso trae consigo las nuevas formas de criminalidad, la especialización de los delincuentes, nacen nuevos tipos delictivos etc. y por ello resulta más costoso su persecución e investigación, nos encontramos con barreras judiciales ante la falta de legislación en estos campos tan novedosos.

Celebrado el vigésimo primero aniversario del Convenio sobre la Ciberdelincuencia, comúnmente conocido como el Convenio de Budapest. Tratado de cooperación internacional que junto a sus diferentes protocolos, se fraguó como metodología legal viva aplicada a la protección de la sociedad frente a estas nuevas formas de cibercriminalidad, con el objetivo de "prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando su tipificación como delito" (Consejo de Europa, 2001); favoreciendo la asunción de un marco legal integral y de cooperación común con el que poder hacer frente de forma satisfactoria a la "detección, investigación y sanción" de los ciberdelitos, junto al desarrollo de novedosas formas de salvaguarda y evidencia electrónica, garantes procesales de los diferentes indicios y pruebas virtuales que se obtengan (Consejo de Europa, 2001).

Para ello, este convenio, prevé una reglamentación que, bajo el principio de proporcionalidad, en connivencia a una estricta supervisión judicial y limitación del ámbito de aplicación y duración de las medidas que procedan, garantice los derechos humanos y libertades de los ciudadanos, estableciendo (Consejo de Europa, 2001):

1. La criminalización de la conducta, que va desde el acceso ilícito, ataques a la integridad del sistema y de los datos hasta el fraude informático y los delitos relacionados con la pornografía infantil.
2. Herramientas de derecho procesal para hacer más efectiva la investigación relacionada con ciberdelitos y la obtención de evidencias electrónicas.
3. Una cooperación internacional más ágil y eficiente.

Sin embargo, tras la promulgación de dicho convenio, no todos los países han mostrado la misma celeridad en su ratificación y aplicación; y se han debido evidenciar diferentes episodios contra la seguridad de las personas y los Estados, para favorecer su correcta implantación; tal y como supuso la presentación internacional que la organización hacktivista Anonymous propició con el "caso WikiLeaks", en dónde difundieron información sensible de varios miembros y departamentos del Gobierno estadounidense, iniciando además una campaña de ciberataques contra diversas multinacionales del país como Amazon o MasterCard, como seña de apoyo a Julian Assange.

En el caso de España, dicho convenio fue ratificado en septiembre del 2010 (BOE, 2010), y posteriormente corregido en noviembre de ese mismo año. Con ello, le prosiguió la entrada en vigor el 23 de diciembre de 2010 de la Ley Orgánica (en adelante, LO) 5/2010 por la que se modificaba el Código Penal de 1995, actualizándose la tipificación de diversos delitos adaptados a las nuevas formas tecnológicas, entre ellos las estafas y daños informáticos.

El 10 de junio de 2011 se puso en práctica dicha ley durante la intervención policial con la que se detuvieron a tres personas acusadas de conformar "la cúpula de Anonymous en

España“, atribuyéndoles además “haber organizado y ejecutado el 18 de mayo del 2011, la operación denominada Spanish Revolution” con la intención de mermar la normal celebración de las elecciones municipales y autonómicas que se celebrarían en España el 22 de mayo del 2011 a través de la realización de un ataque de Denegación de Servicio Distribuido (DDoS) que mediante el envío masivo de 344.944 correos electrónicos, que “afectaron de forma importante al normal funcionamiento” sobre las páginas webs de “la Junta Electoral Central residente en el Congreso de los Diputados, la Unión General de Trabajadores, así como la propia web del Congreso”, junto a la ulterior planificación de su segunda operación bajo el pseudónimo de “V de Votaciones” contra las páginas web de partidos políticos de representación mayoritaria, Partido Popular, Partido Socialista Obrero Español y Convergencia y Unión (Quintana & Tascón, 2018).

Sin embargo, la sentencia judicial condenatoria contra los acusados, basada en las conclusiones planteadas por el Ministerio Fiscal (Alamillo, 2016), fue recurrida por la parte defensora, argumentando varias deficiencias tanto procesales como procedimentales, en primer lugar atribuidas a la vulneración de varios derechos fundamentales relacionados con la cadena de custodia de los efectos intervenidos, y en segundo orden por la ambigua participación de un Agente de policía investido como Agente Encubierto bajo el pseudónimo “Sprocket”, sobre quien recaía la duda de “haberse ganado la confianza de los acusados en conversaciones en redes sociales no estando amparado de la correspondiente autorización judicial, pudiendo haber llegado incluso a la provocación al delito” (Quintana & Tascón, 2018).

Llegados al año 2016, se emitió el fallo a dicho recurso, absolviendo a todos los acusados de los delitos de pertenencia a organización criminal y delito de daños continuado, aceptando como veraces algunas de las deficiencias procesales argumentadas por la defensa, producidas en la cadena de custodia sobre los efectos informáticos que se les intervinieron a los acusados, a pesar de constatarse su participación en las acciones referidas en el sumario.

En relación a la actuación del funcionario policial incardinado como el Agente Encubierto Sprocket, si bien, fue considerada acorde a derecho, sustentando que en un primer momento su actividad se centró en el mero ciber patrullaje de los entornos virtuales, servidores, foros y canales de chat públicos a través de los que se interrelacionaban los integrantes de *Anonymous Hispania*; posteriormente derivó en un contacto mediante chat con los encartados, y una vez observada su conducta criminal, se emitió correspondiente oficio a la Autoridad Judicial, quien le otorgó la condición de Agente Encubierto, bajo la cobertura legal que confiere el artículo 282bis de la Ley de Enjuiciamiento Criminal, en el que se establece que:

Cuando se traten de investigaciones propias de la delincuencia organizada, el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos.

La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente (BOE, 1882).

Sumado a lo anteriormente reseñado, entre los años 2010 y 2012 en el panorama árabe-magrebí emergieron una serie manifestaciones populares, las denominadas “primaveras árabes” en clamor del establecimiento de regímenes democráticos y

mejora de los derechos sociales y humanos de sus habitantes, que sirviéndose de las nuevas formas de comunicación otorgadas por la adopción masiva de las redes sociales, especialmente YouTube, Facebook y Twitter como formas de denunciar la vulneración de sus derechos, y junto a las revueltas ciudadanas, desembocaron en los derrocamientos de los Gobiernos en Túnez, Egipto y Yemen, así como el inicio de una guerra civil en Siria.

Sin embargo, pese a la legitimidad de estos actos, se generó tal clima de crispación, que favoreció la instauración de grupos islámicos salafistas radicales, que no dudaron en secuestrar tales protestas en favor de sus beneficios ideológicos, que coadyuvados por Organizaciones Terroristas de etiología yihadista, obtuvieron un caldo de cultivo ideal para la captación de adeptos con los que poder materializar sus pretensiones filo terroristas. Y es en este sentido, dónde el 29 de junio del 2014, la Organización Terrorista *Ad-Daulat Al-Islamiyah*, (Daesh), a manos de su líder Abu Bakr Al Bagdadi, proclamaron la instauración de un Califato Islámico en Siria e Irak (Rey & Pons, 2015).

Conscientes del poderío mostrado por los entornos virtuales, Daesh no escatimó en valerse de los recursos necesarios que le hicieron conquistar durante varios años este nuevo campo de batalla, el ciberespacio, en dónde floreció toda clase de foros, redes sociales, páginas web, salas de chat, etc. con los que embaucar a todos aquellos sectores de la población proclives a su extremismo ideológico-religioso; y a quienes se imbuía toda clase de sermones, revistas, manuales y material audiovisual con los que una vez radicalizados, se les adoctrinaba como forma previa su integración en la Organización Terrorista. Fruto de ello, miles de combatientes extranjeros (Foreign Terrorist Fighters) reclutados en todo el mundo, emigraron a zona de conflicto sirio-iraquí para la realización de su particular yihad en el camino de Allah (Rey & Pons, 2015).

España, no fue ajena a esta integración en filas yihadistas por parte de sus ciudadanos y residentes, pues ya el ex ministro del Interior Fernández Díaz (2015) cifraba en 115 las personas que habían salido de España hacia tierras del autoproclamado Califato Islámico de Daesh. Presentando más del 75% de los encartados un denominador común en proceso de reclutamiento que se les realizó durante los años 2013 a 2016, Internet; bien a través de un agente reclutador exclusivamente online, o mediante un entorno mixto entre lo físico y lo virtual, según García-Calvo y Reinares (2017).

Derivado de tal avalancha de combatientes desplazados, que decidieron quebrar los valores democráticos de Europa en favor de la yihad de la espada; junto a aquellos otros sujetos que, de forma autónoma y eminentemente dirigida a través de Internet, habían adquirido el adiestramiento necesario en el manejo de armas y explosivos, que les capacitaría para la comisión de un atentado terrorista.

Ante todo ello, y junto a las dificultades con las que el Estado español debía hacer frente a la investigación de aquellas amenazas virtuales complejas como son la pornografía infantil, el phishing, el tráfico de drogas y armas a través de la Dark Web, entre otros; el legislador español en un acto de responsabilidad a la Seguridad Nacional, se vio obligado a tipificar esta novedosa forma de operativa terrorista a través de la reforma llevada a cabo por la Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, incluyendo tales acciones dentro del articulado antiterrorista.

Seguido a ello, el Consejo de Ministros aprobó a través de la Ley 41/2015, de 5 de octubre, la modificación de la Ley de Enjuiciamiento Criminal, como forma de regulación de nuevas medidas para la investigación tecnológica, introduciendo una novedosa figura procesal, El Agente Encubierto Informático, actualizando de esta forma los obsoletos preceptos de esta norma aprobada en 1882, y cuya última reforma data de 1999; en

consonancia a las incipientes, sofisticadas y transnacionales formas de cibercriminalidad (BOE, 1882).

América Latina no ha sido ajena a estos acontecimientos; ya que cumplido el vigésimo aniversario del Convenio de Budapest sobre la ciberdelincuencia, son muchos los Estados de este continente que se han adherido a este convenio 2021 son muchos los Estados de dicho continente que tras su adhesión, forman parte del Convenio de Budapest sobre la ciberdelincuencia (Consejo de Europa, 2021), y acto seguido, retroalimentados de la influencia que en sus ordenamientos se transpone del Derecho penal español, han pasado a regular la figura del Agente Encubierto Informático.

Y para ello, este artículo pretende abordar las características que se le confieren a esta figura procesal de investigación e infiltración policial en los entramados delictivos virtuales, estableciendo su correlación en el Derecho comparado del Agente Encubierto Informático (en adelante, AEI) español con los ordenamientos jurídicos de **Chile y Colombia.**

2. El agente encubierto informático como herramienta de investigación policial en el ordenamiento jurídico español.

2.1. Regulación normativa:

La necesidad de investigaciones encubiertas, a través de agentes encubiertos de la Policía Judicial es indiscutible y tradicionalmente es una figura internacionalmente regulada en los distintos sistemas procesales penales. Los beneficios de incluir en el germen y gestión de la actividad criminal un miembro de la Policía Judicial, compensan los riesgos de intromisiones a la intimidad o compromiso de derechos fundamentales, razón por la que se asegura la concesión, siempre y cuando se cumpla con todos los requisitos previstos por el legislador. Por ello, con las debidas cautelas y garantías en aras a evitar violaciones de derechos fundamentales, la acogida a ésta y otras diligencias de investigación tecnológicas es totalmente positiva (Rey Huidobro, 1999).

La investigación, persecución y averiguaciones criminales tiene una baza importante con esta figura. Sin embargo, la realidad de la implantación y vertiginoso avance de las tecnologías de la información y de la comunicación han provocado la imperiosa necesidad de “entrar en la red”, para evitar, de alguna forma, la perversa ventaja que disfruta la delincuencia respecto a las fuerzas de seguridad. Es evidente que los medios utilizados hasta el momento, relativos a la investigación de la delincuencia que, se sirve de internet como instrumento de la actividad ilícita son un reto para el Estado de Derecho. Tal y como afirma Benítez Ortúzar:

> La mundialización de la economía ha dado lugar a un proceso de expansión de este tipo de criminalidad traspasando las fronteras nacionales, haciendo ineficaces muchos de los instrumentos de investigación utilizados tradicionalmente por el Estado de Derecho para combatir este tipo de delincuencia (Benítez Ortúzar, 2004).

El control de lo que sucede en las redes, en lo concerniente a la investigación criminal se hace patente en España en el año 1996, con el Grupo de Delitos Telemáticos. El Grupo de Delitos Telemáticos nace en el seno de la Unidad Central Operativa de la Guardia Civil, para perseguir los ilícitos penales cometidos o apoyados en las redes. Las patrullas cibernéticas no pueden ser confundidas con el agente encubierto informático, pues estas patrullas operan en los canales abiertos de internet, como un usuario más, pero que no precisan de una identificación y posterior autorización para entrar en un foro determinado y cerrado.

La novedad y avance en las investigaciones se produce con el agente encubierto informático, cuyas necesidades surgen con la complejidad y ocultación de las comunicaciones en la red, la creación de canales cerrados de comunicación, así como la Deep web o la Dark web. La entrada en canales cerrados de comunicación no puede

llevarse a cabo sin identificación y para hacerlo con una identidad falsa, solo puede hacerse con la autorización judicial de agente encubierto informático.

La figura del Agente Encubierto se estableció por primera vez en el ordenamiento jurídico español a través de la reforma que la Ley de Enjuiciamiento Criminal sufrió en el año 1999, imponiendo los límites y requisitos procedimentales que debía presentar dicha medida, en concordancia a la Constitución y leyes españolas; pues la instauración de dicha medida, por sí misma, supondría un severo detrimento de los derechos fundamentales sobre los investigados (Ley Orgánica, 1999). El apartado 6, introducido por la LO 13/2015, regula la posible investigación por parte de agente de la Policía Judicial con una falsa identidad, para poder acceder a comunicaciones en canales cerrados, para los delitos del apartado 4 del art.282 bis LECrim o delitos previstos en el art. 588 ter a LECrim.

Pero antes de adentrarnos en el artículo 282 de la LECRIM, se ha de esclarecer los principios por los que se rige la solicitud de AEI en España para una investigación, los encontramos consagrados en el ordenamiento jurídico existente, en particular los siguientes:

- Principios de necesidad y excepcionalidad; siendo solo válidas las actuaciones necesarias para llevar a buen fin la investigación y siempre y cuando no existan otras menos lesivas de los derechos fundamentales de la persona.

- Principio de proporcionalidad; indicando que los comportamientos ilícitos a los que se va a autorizar a realizar al AEI deben de ser menos lesivos para el bien jurídico protegido (en este caso la seguridad del Estado) que los beneficios o la gravedad del delito o delitos que se van a perseguir.

- Principio de especialidad; que obliga a que esta medida solo pueda ser utilizada para la investigación de conductas que pudieran ser tipificadas como delitos graves.

- Principio de idoneidad; ya que lo que se investigan son conductas realizadas en Internet por ciberdelincuentes amparados en el anonimato que la red ofrece. Para ello, es necesario establecer una relación más o menos duradera con la finalidad de obtener la confianza de los investigados y poder obtener los elementos probatorios que se cometen con la ayuda de las nuevas tecnologías.

- Interdicción de la provocación delictiva; el agente se infiltra para descubrir y desenmascarar una organización ya preexistente, no pudiendo en el curso de la investigación provocar, inducir o facilitar la comisión de ningún ilícito sin la autorización expresa del juez instructor.

No obstante, no es requisito indispensable que esa judicialización sea previa a la solicitud del AEI ya que, si los indicios obtenidos son suficientes y así lo requiere la investigación, ya en el primer oficio dando cuenta al juzgado de guardia de la Audiencia Nacional puede solicitarse esta medida.

El artículo 282 de la LECrim, autoriza al empleo de dicha medida en base a los siguientes supuestos:

1. Cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, a actuar bajo identidad supuesta, y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir a la incautación de los mismos. La identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por periodos 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.

La resolución por la que se acuerde 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.

La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente (Ley Orgánica, 1999).

Prosigue la norma, indicando que aquellos agentes de la policía Judicial, que, de forma voluntaria, hubieran sido erigidos por la Autoridad judicial como agentes encubiertos, bajo identidad ficticia, "podrán mantener dicha identidad cuando testifiquen en el proceso" proveniente de sus actuaciones, siéndole de aplicación además lo expresado en la Ley 19/1994, sobre protección a testigos y peritos en causas criminales (Ley Orgánica, 1994).

Así mismo, la norma establece en su punto 4, un compendio de aquellos delitos propios de la delincuencia organizada, es decir, de un grupo conformado por tres o más personas, que, de forma permanente o reiterada, acuerden la comisión de los siguientes delitos relativos a (Ley Orgánica, 1994):

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

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

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

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

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

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

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

h) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal.

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

j) Delitos de terrorismo previstos en los artículos 571 a 578 del Código Penal.

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

A diferencia de lo previsto en el apartado primero del art. 282 bis LEcrim, solo podrá autorizar la medida un órgano jurisdiccional. No le está dado al Ministerio Fiscal el acuerdo inicial de la medida. Por lo tanto, podrá autorizarse judicialmente 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. Por ende, la autorización judicial habilitante habrá de reunir los requisitos esenciales que informan el conocido test de legitimidad constitucional de las medidas limitativas de derechos fundamentales.

Dicho de otro modo, se habrá de poder inferir la adecuada proporcionalidad que ha de presidir toda afectación legítima de dichos derechos, argumentando la idoneidad de la medida, su necesidad y el debido equilibrio entre el sacrificio sufrido por el derecho fundamental limitado y la ventaja que se obtendrá del mismo (STC 136/2000, de 29 mayo) en función de las específicas circunstancias que rodean la investigación penal en curso. Resolución judicial determinada desde que concurren indicios suficientes que aconsejan la actuación del agente encubierto.

El agente encubierto informático en el Anteproyecto de Ley de Enjuiciamiento Criminal circunscribe su posible autorización a los delitos del art. 355 del mismo texto (Toapanta, 2021):

a) Delitos dolosos castigados con pena igual o superior a tres años de prisión.

b) Delitos relativos a organizaciones y grupos terroristas, delitos de terrorismo, de asociación ilícita, tráfico ilícito de drogas, sustracción de menores, tenencia, tráfico y depósito de armas, municiones o explosivos, trata de seres humanos, cohecho, tráfico de influencias, malversación, corrupción en las transacciones comerciales internacionales, contrabando, blanqueo de capitales y delitos de organización criminal o cometidos en el seno de la misma.

c) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o medio de telecomunicación (Anteproyecto Ley de Enjuiciamiento Criminal, 2021).

Respecto a la autorización judicial de agente encubierto informático, en el párrafo 6 del art. 282 bis LECrim permite tres actividades:

a) entrar en canales cerrados con una identidad falsa;

b) intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido;

c) analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos;

d) captación de imagen y audio, así como su grabación en comunicaciones dentro de esos canales cerrados (Ley de Enjuiciamiento Criminal,1882).

Si bien ya se ha aclarado que la actuación del agente encubierto informático sólo será preceptiva en casos de delincuencia organizada en la que, lógicamente, y por su naturaleza, también entraría el terrorismo. Debido principalmente a las dificultades que se pueden encontrar por la opacidad de estas asociaciones ilícitas. Aunque hemos de citar, que si finalmente se designa un AEI para un determinado caso y no se termina dando una circunstancia agravante por pertenencia a banda organizada en el fallo del juez, la actuación del agente no se verá empañada, tal y como se demuestra en la jurisprudencia española (STS 575/2013 de 28 junio).

Tal y como sostiene D. Diego Díez:

> "estas medidas sólo pueden ser válidamente utilizadas para la persecución de ciertos tipos delictivos, lo que supone incorporar por decisión del legislador el principio de proporcionalidad entre las medidas de investigación y los delitos, sustrayendo a la decisión de las autoridades, incluida la autoridad judicial, la posibilidad de aplicarlas a la investigación de otras conductas" (Diego Díez, 2000).

Asimismo, como señala Villacampa Estiarte "quedan fuera (del listado taxativo de delitos) infracciones que el legislador ha reconocido como propias de la delincuencia organizada" (Villacampa Estiarte, 2013). Ahora bien, parece que, en determinados tipos penales de los enumerados, dicha proporcionalidad podría no sucederse con la misma intensidad que en otros[1]. Buen ejemplo de ello podrían ser determinados delitos contra el patrimonio, entre los que es posible destacar aquellos relativos a la propiedad intelectual.

Ciertamente, dicho juicio de proporcionalidad realizado en abstracto no impide que se articulen correctamente las garantías que informan los estándares constitucionales de limitación de derechos fundamentales. Muy especialmente, tratándose de un medio extraordinario de investigación el carácter

[1] En sentido similar Gimeno Sendra, Manual de Derecho Procesal Penal, ob. cit., pág. 307, cuando afirma que muchos de los delitos tasados en el apartado 4 del art. 282 bis LEcrim, debido a su escasa gravedad cuantitativa, presentan dudas de proporcionalidad en sentido estricto respecto del medio de investigación, y así enumera los arts. 270 a 277 CP, 244, 332 y 334.

subsidiario de la medida y la consideración casuística de las circunstancias concurrentes en la investigación (Guzmán Fluja, 2016). Por ende, la actuación del AEI ha de ser proporcionada a la finalidad de la investigación, y mantenerse en el trascurso de esta.

La garantía de la eficacia de las tareas investigadoras realizadas en red presenta unas circunstancias específicas en cuanto a medios, estructuras y operativa policial, vista la inmediata capacidad expansiva de los efectos dimanantes de los hechos investigados. De esta forma, es posible afirmar la aplicación excepcional de la medida en investigaciones especialmente complejas[2], mediando los oportunos requisitos constitucionales que informan las citadas medidas limitativas de derechos fundamentales.

Todo ello, bajo un criterio estricto de conexidad delictiva entre el delito investigado y las posibles vías de investigación que se van sucediendo conforme avanzan las actuaciones instructoras. Lo cual no significa que la actuación del agente encubierto pueda trascender, encontrándose restringido su ámbito de intervención a un numerus clausus de delitos previstos.

Centrándonos en el agente, el mismo art. 282 bis LECrim, no soluciona el conflicto del agente encubierto físico/informático en lo concerniente a los riesgos de actuación delictiva en la que podrían incurrir, estos miembros de la Policía Judicial. La eventual determinación de comisión de ilícitos se remite a la valoración del juez competente, conforme al principio rector de proporcionalidad. El apartado 5 del art. 282 bis, 5 LECrim advierte "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" (Ley de Enjuiciamiento Criminal,1882).

Para poder proceder penalmente contra el mismo por las actuaciones realizadas a los fines de la investigación, el Juez competente para conocer la causa deberá, tan pronto tenga conocimiento de la actuación de algún agente encubierto en la misma, requerir informe relativo a tal circunstancia de quien hubiere autorizado la identidad supuesta, en atención al cual resolverá lo que a su criterio proceda.

No cabe duda, que al agente encubierto físico/informático se encuentra sumamente expuesto en su investigación, pues las situaciones a las que se enfrenta son en muchas ocasiones imprevisibles y debe actuar con cautela, pues a posteriori el órgano judicial puede valorar una falta de proporcionalidad o una provocación al delito. Habría que interpretar con posterioridad, si se produce una falta de proporcionalidad, un exceso en las actividades permitidas por la figura.

En la nueva regulación del Anteproyecto de LECrim el art. 506 Responsabilidad por conductas delictivas durante la infiltración, refiere de forma sucinta esta cuestión:

1. En ningún caso el agente encubierto podrá instigar, promover o provocar actuaciones delictivas.

2. El agente encubierto estará exento de responsabilidad por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación. Siempre y cuando sean proporcionadas a la finalidad de la medida, no entrañen la lesión a un bien jurídico de mayor valor que el que tratan de proteger y siempre que estén directamente relacionadas con la actividad delictiva de la organización criminal investigada (Anteproyecto de la ley de Enjuiciamiento Criminal, 2021).

[2] Véase Rifá Soler «El agente encubierto o infiltrado en la nueva regulación de la LECrim», en Poder Judicial, 1999, núm. 55, pág. 161.

Como se puede apreciar, el Tribunal Constitucional ha fijado los conceptos necesarios para delimitar una posible provocación al delito. El recurso por parte de la defensa de una provocación al delito, por parte del agente es reiterada, calificando al sujeto investigado como parte pasiva en la decisión de delinquir y al agente como parte activa.

3. Informe de derecho comparado

3.1. AEI CHILE:

Mediante el proyecto de ley ingresado con número de boletín 12192-5, que busca derogar a la anticuada y obsoleta Ley 19.223 sobre delitos informáticos, actualizando la legislación en miras del compromiso adquirido por Chile frente al Convenio de Budapest, (El Gobierno de Chile depositó el 21 de Abril de 2017 en Estrasburgo, Francia, el instrumento de adhesión al Convenio sobre la Ciberdelincuencia del Consejo de Europa) en el cual se busca introducir formalmente al ordenamiento jurídico la figura del "Agente Encubierto en Línea" (nomenclatura específica para referirse al AEI).

En primer lugar, se debe delimitar cómo es entendida la herramienta del agente encubierto "convencional" dentro del ordenamiento jurídico chileno. En rasgos amplios, la figura en estudio ha sido definida doctrinariamente como "aquel funcionario policial que actúa en la clandestinidad, generalmente con otra identidad, que desempeña tareas de represión o prevención del crimen mediante infiltración en organizaciones criminales para descubrir a las personas que las dirigen" (Riquelme, 2006).

También, según ya revisamos, como "aquel funcionario policial que oculta su calidad de policía y se infiltra en la organización criminal, por encargo, y con autorización de su servicio" (Politoff, 1997). Llama la atención como en ambas descripciones se hace hincapié en el concepto de "organización criminal". Este hecho se entiende debido a la naturaleza de los delitos para los cuales originalmente el agente encubierto convencional fue concebido, que en su mayoría son propios de la delincuencia organizada y que muchas veces viene a ser la única posibilidad real de penetrar efectivamente en estos núcleos, pero que presenta inconvenientes a la hora de entender su despliegue en entornos digitales, ya que muchos delitos informáticos en la actualidad prescinden completamente de factores como "organización" o "concierto previo", bastando en muchos casos solamente una persona para su comisión.

Regresando al "Agente Encubierto en Línea", se podría definir su figura como aquel funcionario policial que, autorizado por el Juez de Garantía, a petición del Ministerio Público, se infiltra en canales cerrados de comunicación en internet, con la finalidad de esclarecer hechos que podrían encuadrarse en un tipo penal determinado, y de averiguar la identidad y participación de el o los investigados en la comisión de estos, impidiéndolos o comprobándolos. La forma de infiltración será mediante la utilización de una identidad ficticia, en uso de la cual el agente se relacionará, de la manera más cercana posible, con el o los investigados, pudiendo así ingresar al mundo en que éstos desenvuelven sus actividades eventualmente ilícitas (Bravo Sandoval, 2021). De esta forma, esta definición nos permite desglosar los principales elementos de la herramienta objeto de estudio:

a. Agente encubierto en línea podrá ser todo funcionario policial, lo que en Chile agruparía tanto miembros Carabineros de Chile como a los Policías de Investigaciones;

b. Exigencia de autorización judicial por parte del Juez de Garantía ante la petición del Ministerio Público, en consonancia con el artículo 9 del Código Procesal Penal (Vera, 1883), siempre que la hipótesis sea desplegarlo en canales cerrados de comunicación;

c. Su función será infiltrarse en canales cerrados de internet, con la finalidad de esclarecer hechos que podrían encuadrarse en un determinado tipo penal, además de la identidad y participación de los sospechosos

en la comisión de estos, impidiéndolos o comprobándolos;

d. Su modo de actuar será mediante la ocultación de su identidad como funcionario policial, esgrimiendo una identidad supuesta o ficticia;

e. Procurará establecer una relación de confianza con aquellos individuos que interactúe, con el objeto de que éstos le otorguen acceso a sus canales delictuales y a la información necesaria para perseguirlos penalmente, si es del caso;

f. Su designación tiene carácter de obligatoria respecto del funcionario que desempeñará las labores.

Con relación a lo anteriormente expuesto, cabe valorar por lo tanto que la regulación de funcionamiento del AEI en Chile y España son realmente similares en prácticamente todos los extremos teniendo en cuenta además las vicisitudes propias que cada país tiene en cuanto a su legislación y funcionamiento de sus estructuras policiales y judiciales. Las únicas diferencias destacables son las relativas a la forma de definir sobre qué delitos se puede aplicar esta medida y el tiempo de concesión de la misma.

De esta manera, mientras que en España a través de la última actualización normativa se ha hecho una descripción genérica de delitos que permite abarcar un amplio espectro, en Chile cuentan con una definición mucho más acotada. Asimismo, mientras que en España esta medida es concedida de inicio por un tiempo de seis meses, en Chile tan solo lo es por el periodo de sesenta días.

En lo referente a la legislación del "Agente Encubierto en Línea", cabe mencionar que se halla un tanto disperso por el ordenamiento jurídico chileno, pero se puede mencionar la Ley 20.000, la cual sanciona el tráfico ilícito de estupefacientes y sustancias sicotrópicas, publicada en el Diario Oficial con data 16 de febrero de 2005.

En el inciso segundo de su artículo 25, la Ley 20.000 define la figura en estudio como;

> "aquel funcionario policial que oculta su identidad oficial y se involucra o introduce en las organizaciones delictuales o en meras asociaciones o agrupaciones con propósitos delictivos, con el objeto de identificar a los participantes, reunir información y recoger antecedentes necesarios para la investigación" (Ley 20.000, 2005)

En los siguientes incisos, el mismo artículo trata sobre la posibilidad de otorgar una identidad ficticia al agente, a cargo de la Dirección Nacional del Servicio de Registro Civil e Identificación, así como de la exención de responsabilidad criminal por los delitos en que el agente deba incurrir o no pueda impedir, siempre proporcionales y consecuencia de la investigación. Hasta el proyecto de ley ingresado con número de boletín 12.192-2.560, que busca adecuar nuestra legislación a las prerrogativas del Convenio de Budapest, iniciado en mensaje 164-366 por el presidente de la República –de ahora en más, referido indistintamente como "proyecto de adecuación" o simplemente "proyecto"–, en nuestro ordenamiento jurídico no existe mención específica sobre el actuar del agente encubierto en espacios virtuales (Bravo Sandoval, 2021).

No obstante, podemos señalar la hipótesis tratada por el artículo 369 ter del Código Penal chileno, donde se regula el intercambio de material pornográfico infantil por agentes encubiertos, tales como fotos o videos. Dicho artículo dispone que tanto el actuar del agente como las entregas vigiladas pueden tener lugar a través de un "sistema de telecomunicaciones".

Esta consideración normativa sería la única, en la legislación vigente, en que se referencia el actuar del agente encubierto en un contexto informático de manera explícita (Bravo Sandoval, 2021).

Sin embargo, en su último inciso, el mismo artículo 369 ter del Código Penal finaliza remitiéndose a la normativa de la Ley 20.000 para regir la actuación de los agentes, sin

entregarle una regulación especial. Dicho lo anterior, se hace menester revisar la nueva normativa con que el proyecto de adecuación pretende formalizar la introducción del agente encubierto en línea al ordenamiento jurídico chileno.

El proyecto de adecuación citado establece de entrada que será el Juez de Garantía, a petición del Ministerio Público, el que tendrá la facultad de autorizar la procedencia del agente encubierto en línea, consagrando la necesidad de una autorización judicial habilitante para el despliegue de esta herramienta. El Juez de Garantía, según el inciso primero del artículo 12 del proyecto[3], deberá chequear que:

(I) la medida sea imprescindible en la investigación requerida;

(II) que existan sospechas fundadas sobre el investigado, respecto de que se están cometiendo delitos que hacen procedente el despliegue del agente, y, además;

(III) que el Ministerio Público, de forma previa a solicitar la medida, haya presentado un "informe detallado" respecto de los hechos y la posible participación de los investigados.

Como nos estamos refiriendo a un proyecto de ley, lamentablemente no contamos con jurisprudencia que nos ayude a identificar los elementos que deberá contener la autorización del Juez de Garantía para la concesión de AEI. Así que, para poder enumerarlos, recurriremos a los requisitos establecidos en la normativa del proyecto de adecuación, auxiliándonos además con la Instrucción General[4] que imparte criterios de actuación en delitos de la Ley 20.000, dictada por el fiscal nacional del Ministerio Público mediante Oficio 061/2009, con data de 30 de enero de 2009.

Aunque dicha Instrucción establece requisitos para los fiscales a la hora de designar un agente encubierto "convencional" –ya que como se comentó anteriormente, se requiere de habilitación judicial–, podemos extraer algunos de ellos para enumerarlos. De esta forma, es posible establecer que la autorización judicial habilitante para la práctica del agente encubierto en línea deberá contener (Bravo Sandoval, 2021):

- "Nombre y dirección" del afectado o afectados por la medida investigativa;
- Indicación del tipo de medida y su duración, que no podrá exceder de 60 días, prorrogable por un período de hasta igual duración, si el Juez de Garantía estima que su concurrencia sigue siendo imprescindible y que existen sospechas fundadas;
- Datos que permitan la individualización del agente encubierto y su nombre ficticio o clave bajo el cual se denominará;

[3] Hasta la última modificación hecha al proyecto de adecuación, con fecha 29 de enero de 2021, esta referencia se entendía realizada al primer inciso del artículo 12. Al agregarse el que ahora es el segundo inciso, este pasaje en el proyecto debiese referirse a "los incisos anteriores", y no solo al "inciso anterior", ya que, de ser así, nos quedaríamos sin los requisitos establecidos en el inciso primero para el proceder del agente, es decir, que la medida sea imprescindible, que existan sospechas fundadas sobre los investigados, y la necesidad de presentar un informe previo por parte del Ministerio Público. Además, no se excluirían en la procedencia del agente los delitos contenidos en los artículos 6 y 8 del proyecto de adecuación, ya que también los excluye el inciso primero del artículo 12, a saber, el delito de receptación de datos informáticos y el delito de abuso de dispositivos. La redacción de la norma, que dicta que el agente tiene el fin de "esclarecer los hechos tipificados como delitos en esta ley", haría que todos los delitos tipificados por el proyecto fueran incluidos, de no considerarse el inciso primero. Para efectos del desarrollo de la presente investigación, entenderemos que la referencia a un solo inciso es un error del legislador, considerando los requisitos de ambos incisos para estudiar la procedencia y ámbito de aplicación del agente encubierto en línea.

[4] Dentro de las atribuciones que legalmente corresponden al fiscal nacional, contenidas en el artículo 17 de la Ley Orgánica Constitucional Nº 19.640 del Ministerio Público, se contempla la de dictar instrucciones generales que estime necesarias para el adecuado cumplimiento de las tareas de dirección de la investigación de los hechos constitutivos de delitos, el ejercicio de la acción penal, y la protección de víctimas y testigos.

- Rol único de la causa en la cual será utilizado el agente encubierto, si es del caso;
- Cuerpo policial al que pertenece el funcionario que oficiará de agente encubierto;
- Medidas de protección para el agente que se estimen necesarias en cada caso;
- Mención sobre la habilitación del agente para que éste intercambie y envíe por sí mismo, en el período en que se autorice su despliegue, archivos ilícitos por razón de su contenido;
- Mención sobre la habilitación del agente para que éste obtenga imágenes y grabaciones de las comunicaciones que sostenga con el investigado.

En cuanto al ámbito de aplicación del agente encubierto en línea se limitará al catálogo de delitos establecidos en el inciso primero del artículo 12 del proyecto de adecuación, específicamente a los tipificados en los artículos 1º, 2º, 3º, 4º, 5º y 7º, consagrados en los preceptos que se indican (Corte Suprema, 2019):

a. Delito de ataque a la integridad de un sistema informático, establecido en el artículo 1 del proyecto de adecuación;

b. Delito de acceso ilícito, establecido en el artículo 2 del proyecto de adecuación;

c. Delito de interceptación ilícita, establecido en el artículo 3 del proyecto de adecuación;

d. Delito de ataque a la integridad de los datos informáticos, establecido en el artículo 4 del proyecto de adecuación;

e. Delito de falsificación informática, establecido en el artículo 5 del proyecto de adecuación;

f. Delito de fraude informático, establecido en el artículo 7 del proyecto de adecuación;

Otra diferencia en la legislación chilena respecto de la española es que no existe mención alguna sobre el carácter voluntario que podría tener la designación del agente encubierto –"convencional" o "en línea"– con respecto a la persona que es nombrada, a diferencia de lo estudiado en el derecho español. Sin una norma especial, en Chile extraemos su obligatoriedad a consecuencia de la denominada "obediencia debida".

La "obediencia debida" puede ser entendida, de manera general, como aquella situación en la cual una persona tiene la obligación legal de obedecer a otra, principalmente en organizaciones regidas por el principio jerárquico.

Cuando la orden que se debe obedecer es considerada antijurídica, puede hacerse valer como eximente de responsabilidad criminal, previa representación de la orden ilegal al superior y siempre que este haya insistido en su cumplimiento.

Con ánimo de ordenar de una manera más visual para el lector las principales diferencias entre la regulación chilena y española de la figura del AEI se ha elaborado el siguiente (cuadro I):

CUADRO I

CHILE		**ESPAÑA**
Funcionario Policial	**Designación de AEI**	Funcionario policial miembro de la Policía Judicial
Autorización judicial del Juez de Garantía	**Requisito Judicial**	Autorización judicial del Juez de Instrucción
Identidad supuesta expedida por la Dirección Nacional del Servicio de Registro Civil e Identificación	**Proporción de Identidad**	Identidad supuesta expedida por el Ministerio del Interior
- Organizaciones delictuales - Meras asociaciones o agrupaciones	**Competencias**	- Delitos de terrorismo - Delitos dolosos castigados con pena límite

con propósitos delictivos - Delitos de ataques a la integridad de un sistema informático - Delitos de acceso ilícito - Delitos de interceptación ilícita - Delitos de ataque a la integridad de los datos informáticos - Delito de falsificación informática - Delito de fraude informático		máximo de, al menos, tres años de prisión - Delitos cometidos en el seno de un grupo u organización criminal - Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación
60 días prorrogables por periodos de hasta igual duración	**Concesión**	6 meses prorrogables por periodos de igual duración
Bajo autorización del Juez de Garantía, tenencia e intercambio de archivos ilícitos	**Actuación**	Bajo autorización del Juez de Instrucción, tenencia e intercambio de archivos ilícitos
Identidad y demás datos personales del investigado (domicilio, ocupación, …), así como su rol, actuaciones, grado de participación en los delitos de la causa por la que se abrió investigación	**Objeto de Investigación**	Identidad y demás datos personales del investigado (domicilio, ocupación, …), así como su rol, actuaciones, grado de participación en los delitos de la causa por la que se abrió investigación
Canales o comunidades cerradas y/o abiertas de comunicación.	**Plataformas de Actuación**	Canales o comunidades cerradas y/o abiertas de comunicación.

Fuente: elaboración propia

Con relación a lo anteriormente expuesto, cabe valorar por lo tanto que la regulación de funcionamiento del AEI en Chile y España son cuanto menos, muy similares en prácticamente todos los puntos teniendo en cuenta además las vicisitudes propias que cada país tiene en cuanto a su legislación y funcionamiento de sus estructuras policiales y judiciales.

Entre las únicas diferencias más destacables son las relativas a la forma de definir sobre qué delitos se puede aplicar esta medida y el tiempo de concesión de la misma. También llama la atención, que el papel del AEI en España debe de realizarlo un policía con formación especial miembro de la policía judicial, mientras que en Chile podrá desempeñarlo cualquier funcionario de policía, independientemente del grupo dentro del cuerpo donde se encuentre.

De esta manera, mientras que en España a través de la última actualización normativa se ha hecho una descripción genérica de delitos que permite abarcar un amplio espectro, en Chile cuentan con una definición mucho más acotada. Asimismo, mientras que en España esta medida es concedida de inicio por un tiempo de seis meses, tiempo que aporta al AEI un rango de actuación más amplio, en Chile tan solo lo es por el periodo de sesenta días, aunque cierto es, que ambos países se guardan la posibilidad de prórrogas, siempre bajo informe preceptivo donde exponga los motivos por los cuales se necesite ampliar la investigación y autorización del Juez de Garantía o Instrucción respectivamente.

3.2. AEI COLOMBIA:

No hace muchos años que **Colombia firmó,** como país intencionado**, la adhesión al Convenio sobre la Ciberdelincuencia de Budapest** (Congreso de Colombia, 2018), uno de los principales instrumentos para poder luchar contra la ciberdelincuencia a nivel global y proteger los actos indebidos contra la confidencialidad, disponibilidad e integridad de los sistemas informáticos. Colombia

promulgó la Ley Nº 1928 de 24 de julio de 2018, que aprueba el texto del Convenio de Budapest sobre la Ciberdelincuencia.

Pero antes de comentar dicha ley más específica en materia reguladora del AEI, se procederá a repasar brevemente lo que la Ley 906 de 2004, reguladora de Código de Procedimiento Penal dice al respecto. En materia del Agente encubierto virtual nos debemos situar en su artículo 242 donde expone que la actuación quedará a juicio del Fiscal cuando:

> "tuviere motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado en la investigación que se adelanta, continúa desarrollando una actividad criminal, previa autorización del Director Nacional o Seccional de Fiscalías…En desarrollo de esta facultad especial podrá disponerse que uno o varios funcionarios de la policía judicial o, incluso particulares, puedan actuar en esta condición y realizar actos extrapenales con trascendencia jurídica" (Constitucional, 2004).

Extraemos por tanto una coincidencia total con la regulación española, teniendo que ser un miembro de la policía judicial el encargado de realizar las labores de investigación del Agente encubierto virtual, otra similitud se encuentra en la deliberación de los contextos para designar a un agente encubierto informático (cuando "tuviera motivos razonablemente fundados…continua desarrollando una actividad criminal"), la única diferencia que encontramos es que esa potestad última de autorización recabará en un Fiscal, como ya hemos comentado en España será el Juez de Instrucción, o en determinados casos, el Ministerio Fiscal dando cuenta inmediata al Juez de Instrucción.

Además, debemos de entender que las labores de investigación del Agente encubierto virtual se deben de dar, al igual que en España y Chile, bajo un canal de comunicación muy estrecha entre el propio agente y el fiscal, donde fluya toda información recabada de sus actuaciones, puesto que si seguimos leyendo el artículo 242 aclara que;

si existe información útil para los fines de la investigación, lo hará saber al fiscal para que este disponga el desarrollo de una operación especial, por parte de la policía judicial, con miras a que se recoja la información y los elementos materiales probatorios y evidencia física hallados (Constitucional, 2004).

Si bien se debe matizar, que, a diferencia del Código Penal Español y Chileno, este guarda la posibilidad de que sea un particular, sin modificar su identidad, que ya sea de confianza del imputado, el encargado de colaborar con la justicia en las labores de investigación (Constitucional, 2004).

La Ley los faculta o bien para adulterar su identidad, con el fin de infiltrarse en la organización y ganarse la confianza de sus integrantes para así suministrar información relevante a la persecución penal, o bien –en el caso de los particulares- para actuar "sin modificar su identidad", lo cual presupone que la persona ya "sea de la confianza del indiciado o imputado o la adquiera para los efectos de la búsqueda y obtención de información relevante y de elementos materiales probatorios y evidencia física (Ortiz Rodríguez y Suárez Araque, 2019).

Así también, se contempla que el agente encubierto posee facultades para "intervenir en el tráfico comercial, asumir obligaciones, ingresar y participar en reuniones en el lugar de trabajo o domicilio del indiciado o imputado y, si fuere necesario, adelantar transacciones con él…" (Constitucional, 2004).

A diferencia de la Ley Nº 1928, como veremos a continuación, los tiempos que el Código de Procedimiento Penal baraja para las actuaciones del Agente encubierto virtual son de un año como máximo, pudiendo ser prorrogado por otro más, con debida justificación (Constitucional, 2004).

Aunque se entiende el cambio de los tiempos y la controversia que pueda generar de ello, puesto que la ley reguladora del Código de Procedimiento Penal se sacó en el año 2004, en un contexto histórico determinado, mientras que la ley Nº 1928, se sacó en 2018 como respuesta a la adhesión al Convenio de Budapest y a la necesidad debido al nuevo contexto cambiante por el transcurso de los años (influenciado principalmente por el boom de las nuevas tecnologías) de legislar la actuación del AEI para perseguir determinados delitos que resultan realmente complicados de investigar por su naturaleza y comisión en el seno de las organizaciones criminales.

La presente ley Nº 1928, tal y como describe en su capítulo I, el artículo 1 de la misma, se aplicará en los casos en cuya investigación y judicialización se encuentre la presunta participación de los Grupos Delictivos Organizados (GDO), y los Grupos Armados Organizados (GAO) (Congreso de Colombia, 2018).

En cuanto al referente capítulo sobre medidas punitivas para combatir las organizaciones criminales, cabe destacar también el artículo 4, donde aumentará las penas en una tercera parte cuando las conductas determinadas se produzcan en el seno de los grupos delictivos organizados y grupos armados organizados (Congreso de Colombia, 2018), complementando así su Código Penal, afectando concretamente a su artículo 387 relativo al Constreñimiento del sufragante (Constitucional, 2000). Y es que, en este aspecto encontramos la primera similitud, tanto el ordenamiento jurídico colombiano como el español, en el ámbito penal, concibe la comisión de cualquier hecho delictivo en el seno de una "organización criminal" como una circunstancia agravante de la pena, y no lo tipifica como un delito particular.

Pasando al capítulo II sobre las herramientas de investigación y judicialización, nos encontramos el artículo 12 que complementa al artículo 244A de la ley 906 de 2004 (Constitucional, 2004), donde regula los términos para la realización de actividades investigativas de Grupos Delictivos Organizados y Grupos Armados Organizados, el cual quedaría tal que así:

Sin perjuicio de lo establecido en las normas que prevean un término mayor, en el caso de las actividades investigativas que requieran control judicial previo, cuando se trate de las investigaciones que se adelanten contra miembros de Grupos Delictivos Organizados y Grupos Armados Organizados, la orden del fiscal deberá ser diligenciada en un plazo de seis (6) meses, si se trata de la indagación, y de tres (3) meses, cuando esta se expida con posterioridad a la formulación de imputación (Congreso de Colombia, 2018).

Como breve inciso, y aun suponiendo un salto en la enumeración de artículos, estos tiempos se mantendrán en todo momento a lo largo de la presente ley, con el matiz de la prórroga, que tal y como se expone en el artículo 18, será por tiempos de igual duración (Congreso de Colombia, 2018), al igual que en la regulación chilena y española.

A continuación, en el artículo 13, expone que "los miembros de la policía judicial deberán recabar informes parciales de los resultados de la interceptación de comunicaciones" (Congreso de Colombia, 2018), todo ello con el fin de recolectar evidencias o pruebas materiales probatorias.

En el artículo 16 se declara al igual que en la legislación chilena y la española acerca la figura del AEI, la posibilidad de este para tener y compartir archivos ilícitos siempre y cuando sean necesarios por objeto de su investigación, del mismo modo también podrá "analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos. También obtener imágenes y grabaciones de las conversaciones que puedan mantenerse en los encuentros previstos entre la gente y el indiciado" (Congreso de Colombia, 2018).

En todo caso, a tenor de lo dispuesto en el artículo 22 de la presente ley, la indagación y la información que derive tendrá carácter de

reservado, sólo la Fiscalía tendrá la potestad de revelar las informaciones que estimen oportunas por razones de interés general (Congreso de Colombia, 2018).

Las indagaciones en el ámbito del AEI se verán finalizadas por (Morinelly Lizcano, 2021);

- Cumplimiento de la misión.

- Cumplimiento del término dispuesto por el fiscal, sin que se haya otorgado prórroga.

- Peligro inminente para la vida o la integridad personal del agente o de su familia.

- Cuando la información obtenida carezca de relevancia o la misma pueda obtenerse a través de otros actos de investigación.

- Cesación de la voluntariedad del agente en cubierto.

- Desviación de esta o la identidad del agente encubierto.

- Revelación de esta o la identidad del agente encubierto.

- Incumplimiento de los deberes y obligaciones establecidas.

- Separación o suspensión del servicio público del agente encubierto.

- Muerte del agente encubierto.

Al igual que en el punto anterior, se procede a establecer un cuadro (cuadro II) para tener una comparativa más visual del marco legislativo colombiano y español respecto de la figura del AEI.

CUADRO II

COLOMBIA		**ESPAÑA**
Funcionario Policial miembro de la Policía Judicial, y, excepcionalmente, un particular	**Designación de AEI**	Funcionario policial miembro de la Policía Judicial
Autorización del Fiscal, previa autorización de su director Nacional o Seccional de Fiscalías	**Requisito Judicial**	Autorización judicial del Juez de Instrucción
Bajo autorización del director Nacional o Seccional de Fiscalías, los mismos miembros funcionarios de la Policía Judicial están facultados para adulterar su propia identidad.	**Proporción de Identidad**	Identidad supuesta expedida por el Ministerio del Interior
Cualquier tipo de actividades presuntamente delictivas que se produzcan en el seno de una organización criminal, es decir, grupos delictivos organizados (GDO), y los grupos armados organizados (GAO).	**Competencias**	- Delitos de terrorismo - Delitos dolosos castigados con pena límite máximo de, al menos, tres años de prisión - Delitos cometidos en el seno de un grupo u organización criminal - Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación
1 año prorrogable por 1 año más mediante la debida justificación	**Concesión**	6 meses prorrogables por periodos de igual duración
Bajo control del Juez de Control de Garantías, el agente de la	**Actuación**	Bajo autorización y control del Juez de Instrucción, el agente de la Policía Judicial podrá:

Policía Judicial podrá: - intercambiar o enviar archivos ilícitos por razón de su contenido - analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos. - obtener imágenes y grabaciones de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el indiciado. En cuanto al particular, podrá: - interferir tráfico comercial - asumir obligaciones - ingresar y participar en reuniones en el lugar de trabajo o domicilio del indiciado o imputado - si fuera necesario, adelantar transacciones con él		- intercambiar o enviar archivos ilícitos por razón de su contenido - analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos. - obtener imágenes y grabaciones de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado.
Identidad y demás datos personales del investigado (domicilio, ocupación, …), así como su rol, actuaciones, grado de participación en los delitos de la causa por la que se abrió la indagación	**Objeto de Investigación**	Identidad y demás datos personales del investigado (domicilio, ocupación, …), así como su rol, actuaciones, grado de participación en los delitos de la causa por la que se abrió la investigación
Canales o comunidades cerradas y/o abiertas de comunicación.	**Plataformas de Actuación**	Canales o comunidades cerradas y/o abiertas de comunicación.

Fuente: elaboración propia.

4. CONCLUSIONES

Como se ha podido constatar, en uno y otro caso, las nuevas realidades delictivas que tratan de debilitar las sociedades democráticas, han hecho reaccionar al legislador en el sentido de ofrecer cobertura legal a los miembros de la Policía Judicial cuando desarrollan su actividad profesional mediante la figura del agente encubierto.

Y esto ha de ser así, no sólo en el ámbito de derecho interno, sino que todos los estados deben incorporar a su normativa estatal mecanismos faciliten las investigaciones en sus territorios (armonización normativa), además de crear instrumentos jurídicos ágiles de colaboración para hacer frente común a la transnacionalidad delictiva.

El legislador ha creído necesario introducir en nuestro ordenamiento jurídico la figura del agente encubierto (año 1999), para que los miembros de la Policía Judicial puedan hacer uso de técnicas de investigación especiales. Esto se produjo porque las metodologías tradicionales se creyeron insuficientes para hacer frente a la delincuencia organizada transnacional.

Más adelante (año 2015), ante el incremento de la actividad delictiva en entornos informáticos, de nuevo, se crean *ex* novo, medidas jurídicas eficaces al objeto de que los investigadores, en la modalidad de agente encubierto informático, pudiesen desarrollar su actividad policial en entornos cerrados de comunicación.

Claro está, que muchos estados bien por incapacidad interna o falta de interés en insertarse en la comunidad internacional para hacer un frente común, no sólo permiten que ciertas actividades criminales partan de sus territorios, delitos de carácter cibernético, sino que los propios autores se mantienen ajenos a una respuesta punitiva dada la incapacidad de un Estado, por sí solo, pueda extender su poder más allá de sus límites territoriales.

Los factores que determinan si nos encontramos ante la técnica policial de investigación criminal en ámbitos de criminalidad organizada, donde opera el agente encubierto, son tres: ocultar la verdadera identidad, que se trate de agente de la Policía Judicial, y que se infiltre en la organización criminal para la averiguación y puesta a disposición judicial no sólo del autor/es del entramado criminal, sino de desmantelar la propia organización.

Así, la técnica especial de investigación, bajo la modalidad de agente encubierto se ofrece como herramienta eficaz en contextos de crimen organizado, así como las diferentes modalidades delictivas graves que utilizan como soporte la red. Y aunque el fin último, es la detención de los presuntos delincuentes que cometen la actividad criminal como se ha dicho, no lo es menos, si cabe mayor, desvelar el modo en cómo se organiza la organización, su *modus* operandi, además del alcance e implicaciones de sus actividades criminales.

Conscientes de las implicaciones y consecuencias que acarrea entrometerse en la jurisdicción de otro Estado, la creación de entornos supraestatales de investigación no son una alternativa, sino una necesidad.

De esta forma, como se ha desarrollado en el texto, tanto en contextos territoriales que afectan a los miembros de la Unión Europea, como de terceros estados, existen posibilidades de actuar conjunta y coordinadamente en escenarios distintos, incluso con el valioso apoyo de las agencias Europol como Interpol.

Desde luego, el aunar esfuerzos conjuntos en pro de erradicar la delincuencia transnacional ha de entenderse como una necesidad estratégica, en tanto el incremento de este tipo de actividades se conviertan en sistémicas, y puedan debilitar las estructuras del Estado, incluso, extenderse a la sociedad en el sentido de ofrecerse como una lucrativa forma de vivir.

Referencias

BENÍTEZ ORTÚZAR, Ignacio. F. (2004). El colaborador con la justicia. Aspectos sustantivos, procesales y penitenciarios derivados de la conducta del «arrepentido», Dykinson.

BRAVO SANDOVAL, Carlos. (2021). El agente encubierto en línea: principales características, derecho comparado, y desafíos que subyacen a su regulación. https://repositorio.uchile.cl/handle/2250/180210

CASTELLS, Manuel. (2006). La sociedad red: una visión global. Alianza Editorial, p. 56.

DIEZ, De Diego. (2000). «Especialidades de la declaración testifical: agentes encubiertos; confidentes y testigos de referencia», en El Proceso Penal. Tirant lo Blanch.

GINER ALEGRÍA, Cesar. Augusto., & DELGADO MORÁN, Juan. José. (2017). Consideraciones criminológicas sobre el perfil del stalker y el acecho mediante ciberstalking. *Estudios en seguridad y defensa*, 12(24), 19-35. https://doi.org/10.25062/1900-8325.250

GONZÁLEZ TRIGO, Norberto Aser. (2023). El agente encubierto ante la criminalidad organizada transnacional. *Cuadernos de RES PUBLICA en derecho y criminología*. (1) (mayo): 85-94. https://doi.org/10.46661/respublica.8062

GUZMÁN FLUJA, Vicente Carlos. (2016). El agente encubierto y las garantías del proceso penal, en Publicaciones del Portal Iberoamericano de las Ciencias Penales Instituto de Derecho Penal Europeo e Internacional.

MARTINO, Luigi. (2024). International Law, State Sovereignty and Competition in the Digital Age. *Rivista di filosofia del diritto internazionale e della politica globale*, Vol. 21, Nº. 2,

MARTINO, Luigi., PAYÁ SANTOS, Claudio. Augusto & DELGADO MORÁN, Juan, José. (2024). Thus,do they all: APTs as instruments of State-Sponsored cyber operations. *Eksploriump*. V. 45 No. 1s, 27-50. https://doi.org/10.52783/eksplorium.145

MAZURIER, Pablo, Andrés., DELGADO MORÁN, Juan, José & PAYA SANTOS, Claudio, Augusto. (2019). Gobernanza constructivista de la internet. *Teoría y Praxis*, 17(34), 107-130. https://doi.org/10.5377/typ.v1i34.14823

MORINELLY LIZCANO, Julio. Hernan. (2021). Actuación del agente encubierto virtual como técnica especial de investigación criminal. https://hdl.handle.net/10901/20495

ORTIZ RODRÍGUEZ, María, Paula., y SUAREZ ARAQUE, Dayana. Andrea. (2019). El agente encubierto, una mirada desde la jurisprudencia colombiana. https://hdl.handle.net/10901/19126

PAYÁ SANTOS, Claudio. Augusto, DELGADO MORÁN, Juan. José;. MARTINO, Luigi; GARCÍA SEGURA, Luis, A.; DIZ CASAL, Javier, & FERNÁNDEZ RODRÍGUEZ, Juan, Carlos. (2023). Fuzzy Logic analysis for managing Uncertain Situations. Review of Contemporary Philosophy Vol 22 (1), 2023 pp. 6780 -6797. https://doi.org/10.52783/rcp.1132

POLITOFF LIFSCHITZ, Sergio. (1997). El agente encubierto y el informante infiltrado en el marco de la Ley 19.366 sobre tráfico ilícito de estupefacientes y sustancias sicotrópicas. *Gaceta Jurídica,* N°203.

QUINTANA, Yolanda., y TASCÓN, Mario. (2018). Ciberactivismo: Las nuevas revoluciones de las multitudes conectadas. Los Libros de la Catarata.

REY HUIDOBRO, Luis. Fernando. (1999). El delito de tráfico de drogas. Aspectos penales y procesales, Tirant Lo Blanch.

REY, Matthieu. (2015). Sobre los orígenes del Estado Islámico. *Pasajes: Revista de pensamiento contemporáneo*, (47).

REINARES NASTARES, Fernando, GARCÍA CALVO, Carola y VICENTE, Álvaro. (2017). Dos factores que explican la radicalización yihadista en España, Real Instituto Elcano.

RIQUELME PORTILLA, Eduardo (2006). El agente encubierto en la ley de drogas. La lucha contra la droga en la sociedad del riesgo. *Revista Política Criminal,* (2).

RODRÍGUEZ GONZÁLEZ, Víctor., PAYÁ, SANTOS, Claudio, Augusto., & PEÑA HERRERA. Bernardo. (2023). Estudio criminológico del ciberdelincuente y sus víctimas. *Cuadernos de RES PUBLICA en Derecho y criminología,* (1) 95-107. https://doi.org/10.46661/respublica.8072.

RUBIO ALAMILLO, Javier. (2016). Conservación de la cadena de custodia de una evidencia informática. *Diario La Ley*, (8859)

FUSTER-FABRA TOAPANTA, J. Ignacio., & VELASCO SÁNCHEZ, José. Carlos. (2021). Anteproyecto de Ley de Enjuiciamiento Criminal. In El impacto de la oportunidad sobre los principios procesales clásicos: Estudios y diálogos Iustel.

VERA, Robustiano. (Ed.). (1883). Código penal de la República de Chile. P. Cadot i ca.

VILLACAMPA ESTIARTE, Carolina (2013). La delincuencia Organizada: Un reto a la Política Criminal Actual, Thomson Reuters Aranzadi.

REFERENCIAS JURÍDICAS:

Boletín Oficial del Estado, (1882). Ley de Enjuiciamiento Criminal. Madrid: Ministerio de la Presidencia. Retrieved December, 10, 2006.

Boletín Oficial del Estado [BOE], 17 de septiembre de 2010. Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

Boletín Oficial del Estado [BOE], 14 de octubre de 2010. Corrección de errores del Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

Congreso de Colombia (2018). Ley N.º 1928 de 24 de julio de 2018, que aprueba el texto del Convenio de Budapest sobre la Ciberdelincuencia. Ministerio de Asuntos Exteriores.

Consejo de Europa (2001). Convenio sobre la ciberdelincuencia. Serie de Tratados europeos nº 185.

Consejo de Europa (2021). Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios.

Constitucional, C. (2000). Código Penal Colombiano (ley 599 de 2000). Bogotá., Colombia.

Constitucional, C. (2004). Ley 906 de 2004, Código de procedimiento penal. Colombia: Legis.

Corte Suprema, "Oficio n°23-2019", Informe proyecto de ley n° 2-2019", documento de tramitación legislativa, Santiago, 12 de febrero de 2019.

Ley, N. (2005). 20.000, Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas. Santiago, Chile.

Ley Orgánica 19/1994, del 23 de diciembre de Protección a Testigos y Peritos en causas criminales. Boletín Oficial del Estado, 307, 38669-38671.

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. Boletín Oficial del Estado, 275, 38389-45671.

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la LO 10/1995 de 23 de noviembre, del Código Penal, BOE 23 de junio. Boletín Oficial del Estado, 145, 383979-389912.

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, GAZ núm. 260 (1882), BOE-A-6036 (1882).

SENTENCIA 136/2000, de 29 de mayo. BOE núm. 156, de 29 de mayo de 2000.

Sentencia Penal Nº 575/2013, Tribunal Supremo, Sala de lo Penal, Sección 1, Rec 11276/2012 de 28 de junio de 2013.