UNIVERSIDAD DE CHILE

Facultad de Derecho
Departamento de Derecho Procesal

EL AGENTE ENCUBIERTO EN LÍNEA

PRINCIPALES CARACTERÍSTICAS, DERECHO COMPARADO, Y DESAFÍOS QUE SUBYACEN A SU REGULACIÓN

Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales

AUTOR:
CARLOS BRAVO SANDOVAL

PROFESOR GUÍA:
ÁLVARO ALIAGA GREZ

Santiago, Chile
2021

RESUMEN

En la presente investigación, se abordan las distintas implicancias político-criminales que devienen como consecuencia del progreso de las tecnologías, y en torno a esta idea, se plantea la necesidad de una modernización en cuanto a las técnicas investigativas con las que se hace frente a este fenómeno. De esta forma, el agente encubierto se constituye como una poderosa herramienta de indagación, pero desplegado en otro medio: aquel donde su campo de actuación ya no está circunscrito a un espacio físico, sino que salta al mundo digital y se infiltra en internet, cambiando de esta forma algunos elementos configurativos en relación a su figura tradicional.

A consecuencia de este punto, el primer capítulo del trabajo se enfoca en el estudio de la legislación española, la que transcurriendo el año 2015, insertó formalmente en su ordenamiento jurídico la figura del agente encubierto informático. Junto con el análisis de sus elementos fundamentales, se revisan los principales conflictos doctrinarios y jurisprudenciales suscitados en su aplicación desde su entrada en vigencia.

En el segundo capítulo, el trabajo se enfoca en el ordenamiento jurídico chileno, ya que mediante el proyecto de ley ingresado por el Senado con número de boletín 12192-25, de 25 de octubre de 2018, se pretende incluir formalmente en nuestro derecho la figura del agente encubierto en línea. En virtud de esto, la presente investigación se encarga de desmenuzar cada uno de sus elementos, junto con adelantarse a determinados conflictos que podrían suscitarse en su aplicación una vez que sea aprobado, en congruencia a la legislación vigente y lo estudiado en el derecho comparado.

Finalmente, el epílogo de la investigación se encarga de sistematizar las conclusiones derivadas del estudio de este moderno instrumento indagatorio, así como las principales críticas al proyecto de ley chileno referido que continúa en tramitación, según estas palabras son redactadas.

ÍNDICE

RESUMEN 3
ÍNDICE 4
INTRODUCCIÓN 5
CAPÍTULO I: España y el agente encubierto informático 12
1. Concepto 12
2. Legislación 13
3. Procedencia 14
4. Ámbito de aplicación 16
5. Canales de actuación 20
5.1. Actuación en canales de comunicación cerrados 21
5.2. Actuación en canales de comunicación abiertos 21
6. Herramientas de actuación 22
6.1. Intercambio de archivos ilícitos 23
6.2. Análisis de resultados algorítmicos en archivos ilícitos 26
6.3. Grabación de imágenes y sonidos 26
6.4. Exención de responsabilidad criminal 27
CAPÍTULO II: Chile y el agente encubierto en línea 29
1. Concepto 29
2. Legislación 32
3. Procedencia 34
4. Ámbito de aplicación 39
5. Canales de actuación 41
5.1. Actuación en canales de comunicación cerrados 42
5.2. Actuación en canales de comunicación abiertos 42
6. Herramientas de actuación 43
6.1. Intercambio de archivos ilícitos 44
6.2. Grabación de imágenes y sonidos 48
6.3. Particularidades en torno a la consumación del delito 48
6.4. Exención de responsabilidad criminal 49
EPÍLOGO 51
BIBLIOGRAFÍA CONSULTADA 56

INTRODUCCIÓN

Internet ha demostrado ser un fenómeno totalmente revolucionario, que se ha insertado en nuestra cotidianidad hasta un punto más allá de lo que podemos discernir a simple vista. La tecnología, de manera veloz y exponencial, se amalgama cada vez más con nuestras vidas, acompañando y contribuyendo al desarrollo del ser humano en la modernidad. Esta idea alcanza tal magnitud, que actualmente la expresión e interacción de las personas en espacios virtuales es inclusive más amplia que en el espacio físico, tendencia que pareciera no cambiar, condicionando todos los ámbitos de la sociedad contemporánea: cultura, economía, relaciones sociales y en lo que nos compete, al Derecho.

Este escenario, de manera reciente, ha experimentado un fulminante crecimiento producto de la pandemia por Covid-19. Situándonos en el contexto nacional, en Chile existen 3,6 millones de accesos a internet fija, con un crecimiento anual de 5,5%. Además, un 32,8% de estos accesos son mediante la tecnología de fibra óptica[1]. La Subsecretaría de Telecomunicaciones indicaba, a finales de marzo de 2020, que nuestro país experimentaba un 40% más de tráfico total de datos mediante el uso de internet, proyectando un aumento de hasta un 60% para el resto de aquel año[2]. En el contexto internacional, el *Global Digital 2019 reports* revela que el número de personas usando internet ha aumentado de manera exponencial a lo largo de la última década, con más de un millón de nuevos usuarios al día desde enero de 2018[3], entre otros aspectos. En palabras del sociólogo Manuel Castells, la "sociedad red" es el paradigma tecnológico de nuestro tiempo[4], 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. Nos encontramos viviendo un período histórico revolucionario, que a diferencia de anteriores revoluciones comunicacionales, como la invención de la imprenta o el teléfono, es particularmente ágil en cuanto a la distribución de datos y posee una gran capacidad auto-expansiva.

[1] CARRIZO, Emiliano. El consumo de internet se dispara en Chile [en línea]. Santiago, Chile: La Tercera Online, 5 de octubre de 2020. Disponible en: https://www.latercera.com/pulso/noticia/consumo-de-internet-sube-durante-este-primer-semestre-y-el-uso-de-datos-para-jugar-se-dispara-mas-del-100/ [fecha de consulta: 10 de noviembre de 2020].
[2] Subsecretaría de Telecomunicaciones de Chile [en línea]. Santiago, Chile: Página web Subsecretaría de Telecomunicaciones, 2020. Disponible en: https://www.subtel.gob.cl/trafico-total-de-internet-fija-y-movil-crece-40-a-marzo-de-2020-impulsado-por-la-pandemia-de-covid-19/ [fecha de consulta: 9 de septiembre de 2020].
[3] KEMP, Simon. Digital 2019: Global internet use accelerates [en línea]. WeAreSocial.com, 30 de enero de 2019. Disponible en: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates/ [fecha de consulta: 10 de noviembre de 2020].
[4] CASTELLS, Manuel. *La sociedad red: una visión global*. Madrid, España, Alianza Editorial, 2006, p. 56.

Las Tecnologías de la Información y la Comunicación[5] –de ahora en más, denominadas como TICs– son protagonistas y componen los cimientos de la actual revolución tecnológica. Han significado un cambio considerable y cualitativo en nuestro diario vivir, redefiniendo los modos en que interactuamos como sociedad. Sin embargo, también han sentado las condiciones ideales para el cobijo de un nuevo espacio donde la actividad delictiva, de manera discreta y efectiva, puede desarrollarse aprovechando la vertiginosa evolución de las ciencias y la inevitable dilación del legislador.

En este orden de ideas, la masificación del uso de internet tanto en redes privadas como públicas, junto a la utilización civil y empresarial de sistemas informáticos que importan el empleo de ordenadores, teléfonos y todo tipo de dispositivos "inteligentes" que se encuentran conectados a la red, configuran los elementos ideales para la aparición de ingeniosas conductas que no podían ser ideadas sino hasta el día de hoy y que atentan contra bienes jurídicos relevantes y merecedores de protección. Además, las TICs han posibilitado nuevos mecanismos de ejecución respecto de conductas ilícitas convencionales, ya tipificadas en la mayoría de los ordenamientos jurídicos, pero que descubren nuevos medios para llevar a cabo sus propósitos de manera más rápida y eficaz. Una vez insertas en la denominada "sociedad red", las personas no perciben necesariamente estar circunscritas a alguna jurisdicción o nacionalidad en específico, lo cual potencia la sensación de impunidad dentro de ella, a su vez amparada en la infinidad de posibilidades y canales de actuación que la tecnología ofrece.

Naturalmente, Chile no ha estado indiferente a este fenómeno, lo que sumado al impacto de la pandemia por Covid-19, ha evidenciado falencias que abarcan diversas aristas de nuestra sociedad. En lo que nos atañe, se ha destacado la proliferación del crimen con un factor común: el uso de la web como herramienta para su comisión[6]. Si lo llevamos a cifras, la actividad ilícita a través de internet genera un impacto económico aproximado de un billón de euros al año, lo que equivale al PIB de ciertos países europeos, como España. Por otro lado, el gasto en inversión por concepto de ciberseguridad en el mundo, se estima alcanzar tan solo 70.000 millones de euros aproximados[7]. En efecto, el hecho de que la amenaza de la delincuencia en el ciberespacio sea silente no le resta magnitud, y todas estas cifras no han hecho más que agudizarse producto de la pandemia.

[5] Este concepto se refiere al conjunto de tecnologías que permiten acceso, producción, tratamiento y comunicación de información en el formato en que se presente, sea texto, imagen o sonido. El elemento más representativo de las nuevas tecnologías es el computador, y en concreto, la internet.

[6] MENDÍA, Rosario. "Delincuentes de la web: La pandemia como escenario favorable". En: *La Tercera*, Santiago, Chile, 16 de mayo de 2020.

[7] ÁLVAREZ, Luis. Así funciona la ciberdelincuencia, el negocio ilícito más lucrativo [en línea]. Madrid, España: El Mundo, 2017. Disponible en: https://www.elmundo.es/economia/2017/01/08/586fc1d222601d6f4b8b4584.html [fecha de consulta: 12 de noviembre de 2020].

En atención a lo expuesto, alcanzamos el concepto de "**ciberdelito**" o "**delito informático**" –como se emplea con mayor frecuencia en la generalidad de los países de habla hispana[8]– y que podemos definir como "aquella actividad ilícita o abusiva que se relaciona con los ordenadores y redes de comunicación en sentido amplio, ya sea porque: (i) el ordenador se utilice como herramienta del delito, o bien porque (ii) el sistema informático o sus datos, sea el objeto del delito"[9]. Esta última expresión debemos entenderla referida a la de "objeto *material* del delito", concepto que, en oposición al de "objeto *jurídico* del delito", es precisado en doctrina como la persona o cosa sobre la cual recae directamente el daño causado por el delito cometido.

Con el pasar de los años, el catálogo de delitos informáticos con ayuda del vertiginoso avance de las TICs, no hace más que aumentar. Dentro de las nuevas figuras que han adquirido mayor relevancia, encontramos: el "*phishing*", que consiste en la suplantación de identidad mediante el envío de correos electrónicos con apariencia confiable, que finalmente derivan en sitios web fraudulentos dedicados a recabar datos confidenciales de las víctimas. Relacionado al delito de abuso sexual infantil, resalta la figura del "*childgrooming*", definido como una serie de conductas realizadas por una persona mayor de edad, utilizando internet y en la mayoría de los casos redes sociales, para atraer a menores de edad con el propósito de crear una conexión emocional, obtener imágenes íntimas, o bien posibilitar un eventual contacto personal con éstos. Finalmente encontramos el "*pharming*", que consiste en la explotación de una vulnerabilidad en el *software* de los servidores DNS[10] o en el de los equipos del propio usuario, con la finalidad de posibilitar al atacante la redirección de un nombre de dominio web a otro distinto, montado previamente por éste y sin conocimiento de la víctima, donde recopila distintos datos sensibles de ésta mediante el engaño. Además, como ya fue enunciado, ciertas conductas se han visto "revitalizadas" gracias a las TICs: desde delitos como el tráfico de estupefacientes, que recientemente se ha masificado mediante el "*delivery*" de droga[11], hasta conductas menos lesivas pero que adquieren nuevas características y consecuencias, como la migración del *bullying* a escenarios virtuales. Todas estas actividades, en conclusión, se desarrollan hoy con mayor alcance y extensión, a la vez que el medio virtual en que esto ocurre dificulta su persecución penal.

[8] VELASCO, Cristos. *La jurisprudencia y competencia sobre delitos cometidos a través de cómputo e internet*. 1ª ed., España, Tirant Lo Blanch, 2012, p. 50.
[9] MITCHSONI / URRY. "Delitos y abusos en el comercio electrónico". En: *The IPTS Report*, Centro Común de Investigación de la Comunidad Europea, 2001, págs. 19-24.
[10] Se denomina "servidor" a todo equipo informático que forma parte de una red y provee servicios a otros equipos, denominados "clientes". Una de sus muchas funciones, consiste en alojar páginas web. Por otro lado, el Sistema de Nombres de Dominio (o DNS) provee la nomenclatura para poder acceder a estos servidores.
[11] VILLARROEL, María José. Detienen a acusado de realizar "delivery" de droga [en línea]. Santiago, Chile: Radio Bio Bio, 2020. Disponible en: https://www.biobiochile.cl/noticias/nacional/region-metropolitana/2020/07/09/detienen-acusado-realizar-delivery-droga-intento-atropellar-pdi-fiscalizacion-rm.shtml [fecha de consulta: 9 de septiembre de 2020]. PLACENCIA, Felipe. Carabineros de Concepción captura banda que vendía con método "delivery" [en línea]. Concepción, Chile: Diario Concepción, 2020. Disponible en: https://www.diarioconcepcion.cl/ciudad/2020/07/08/carabineros-de-concepcion-captura-banda-que-vendia-droga-con-metodo-delivery.html [fecha de consulta: 9 de septiembre de 2020].

Es menester además mencionar un factor estrechamente relacionado con las víctimas que debemos tener en cuenta. Al año 2015, el Ministerio del Interior de España, mediante un estudio denominado "Estadística de Cibercriminalidad", contabilizaba **60.154** denuncias relacionadas a delitos cometidos mediante el uso de la tecnología, lo que en suma no constituye ni siquiera el 10% del total de delitos que efectivamente se cometen[12]. En lo que respecta a las víctimas del cibercrimen, la ayuda que éstas puedan entregar a las autoridades viene a ser muchas veces determinante, pero lamentablemente no ocurre en la gran mayoría de los casos. La contundente "cifra negra", referida a delitos no denunciados, refleja que las personas no reconocen su condición de víctima, y en consecuencia no denuncian o no perseveran en sus pretensiones procesales. Como aseveramos, el rasgo fundamental de la "sociedad red" es el poderoso carácter anónimo con que allí se actúa, lo que asienta en las víctimas la idea de que la justicia no podrá encontrar responsables o le será excesivamente dificultoso hacerlo. Son los supuestos referidos a la "invisibilidad del delito informático", que se explica por la relatividad espacio/tiempo con que el delincuente actúa en escenarios digitales[13].

En línea con lo anterior, se describe el caso de grandes conglomerados o empresas privadas que son víctimas de ataques informáticos y que se enfrentan a la disyuntiva de realizar o no una denuncia ante la respectiva autoridad, considerando las consecuencias que devienen necesariamente del hecho de realizarla y que se materializan en una "mala imagen" comercial, sumada a la presión intrínseca que significa ser parte de una investigación criminal. Los incidentes en la web suelen asociarse al nivel de seguridad informática que posee la empresa atacada, lo que genera descrédito en la fiabilidad de la gestión misma de su personal en caso de ser publicados. De esta manera, por decisión de las propias víctimas, un amplio número de incidentes en materias de seguridad web transcurren fuera del conocimiento público[14].

La colaboración internacional respecto de la jurisdicción aplicable, disponibilidad de recursos, infraestructura necesaria y disposición de personal técnicamente capacitado para realizar una investigación de naturaleza digital vienen a significar los principales desafíos jurídicos que subyacen ante todo el escenario descrito, vinculados a la aplicación y ejecución de la legislación penal por parte de las autoridades y agencias gubernamentales. Internet cuestiona y quebranta los principios de derecho internacional y aquellas normas tradicionalmente aplicadas por la justicia. Delitos informáticos

[12] ROJAS, Elisabeth. Entrevista a Silvia Barrera, Jefa de la Sección Técnica del Grupo de Investigación en Redes de la Unidad de Investigación Tecnológica (UIT) del Cuerpo Nacional de Policía [en línea]. España: McPro, 2017. Disponible en: https://www.muycomputerpro.com/2017/03/17/silvia-barrera-cnp [fecha de consulta: 13 de noviembre de 2020].
[13] REYNA, Luis. "La víctima en el delito informático". En: *Revista peruana de doctrina y jurisprudencia penal*, N°1, Lima, Perú, 2002, p. 8.
[14] HERRERA, Myriam. "El fraude informático. Actualidad penal". En: *Actualidad penal*, N°39, España, 2001, p. 932.

como el *hacking*, ataques sobre denegación de servicio –DoS o DDoS[15]– y ciberataques terroristas, requieren de la cooperación internacional si quiere verdaderamente hacérseles frente[16].

Ante lo descrito, y dentro de los principales esfuerzos internacionales en la materia, podemos mencionar al **Convenio sobre Ciberdelincuencia del Consejo de Europa**, suscrito el 23 de noviembre de 2001 en la ciudad de **Budapest** –más conocido como *Convenio de Budapest*– que busca establecer una legislación penal y procedimientos comunes entre los países suscriptores, para perseguir delitos cometidos a través de medios electrónicos e informáticos, y al mismo tiempo, fomentar y fortalecer la cooperación internacional en esta materia. El Convenio considera el factor transfronterizo de la ciberdelincuencia, así como la importancia de la prueba digital en su persecución. Si bien la iniciativa del Convenio es europea, su suscripción también ha quedado abierta a estados invitados. El Comité de Ministros del Consejo de Europa, con fecha 18 de junio de 2009, extendió formalmente una invitación a Chile para formar parte del tratado. Finalmente, el día 16 de mayo de 2016 es ingresado al Congreso, siendo promulgado el 27 de abril de 2017 mediante el Decreto Supremo N° 83 del Ministerio de Relaciones Exteriores.

Según su Reporte Explicativo[17], el Convenio se enfoca en el desarrollo y fomento a la utilización de las TICs, así como en manifestar la necesidad de aplicar una política penal común para perseguir esta clase de delitos. Sus finalidades primordiales son: (i) armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos; (ii) establecer conforme al derecho procesal penal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico; y (iii) establecer un régimen rápido y eficaz de cooperación internacional.

Actualmente, para poder enfrentar el fenómeno de la cibercriminalidad, las legislaciones del mundo cuentan con técnicas especiales de investigación que logran auxiliar en este cometido. No obstante, ante la sofisticación informática y material de las organizaciones criminales, y ya no solo de "organizaciones", sino que además de personas que alrededor del mundo y de forma individual, encuentran en el cibercrimen un área prolífica económicamente, se precisa una puesta al día en

[15] Se denomina "ataque de denegación de servicio", también llamado ataque "DoS" –en inglés, *Denial of Service*–, aquel ataque informático a un determinado sistema de redes que ocasiona una caída del servicio para sus usuarios. Usualmente genera la pérdida del control sobre la red mediante la sobrecarga de sus recursos. Una ampliación del ataque "DoS", es el llamado "ataque de denegación de servicio distribuido", también llamado "DDoS" –en inglés, *Distributed Denial of Service*–, el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino, usualmente a través de *bots*, y que asimismo, genera la sobrecarga de los recursos del sistema.
[16] VELASCO, ob. cit., p. 23.
[17] Reporte Explicativo del Convenio sobre Ciberdelincuencia del Consejo de Europa, párrafo 16.

nuestras herramientas de indagación criminal. Existe una profesionalización de la ciberdelincuencia a escala global, lo que ha aumentado progresivamente la cantidad de individuos que delinquen en solitario y, por otro lado, ha complejizado las estructuras de funcionamiento de la criminalidad organizada, cuya principal característica hoy es precisamente su mayor disposición de recursos materiales y humanos en comparativa a lo que podíamos encontrar tiempo atrás[18].

Teniendo en cuenta el potente factor de anonimato en que se funda el vasto mundo de internet y la alta cifra negra de delitos no denunciados, tal como hemos analizado hasta acá, se genera la necesidad de encontrar medidas de persecución criminal que de alguna u otra forma ayuden a mitigar estos elementos y faciliten la imputación de estas figuras penales informáticas. Con la mira en las acciones que pueden llevar a cabo nuestros cuerpos policiales, podemos estudiar una tradicional y polémica figura que viene a solucionar el conflicto planteado: **el agente encubierto**, pero desde otro prisma, trasladado a entornos virtuales donde necesariamente debe cambiar ciertos elementos, alterando en parte algunos de sus atributos.

Situándonos en doctrina nacional, el profesor Sergio Politoff define al agente encubierto 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"[19]. Esta controversial figura debe su empoderamiento a las necesidades político criminales que han surgido en los estados democráticos contemporáneos. Su activo funcionamiento en el orden procesal penal aparece legitimado por la proporcionalidad de éste frente al poder de las organizaciones criminales, así como en función de los bienes jurídicos que busca proteger. Su existencia tensiona la relación que existe entre el deber del estado de resguardar los derechos fundamentales y la necesidad persecutoria penal de contar con herramientas útiles en el esclarecimiento de los delitos.

El desempeño del agente encubierto, lejos de ser emplazado por las TICs, debe ser asistido por éstas, explotando todas las virtudes de la era moderna para lograr los fines de su acción. Los medios tecnológicos nos permiten estar presentes en el mismo espacio virtual en que los delincuentes digitales actúan, de manera sigilosa y cauta, pudiendo constatar, escuchar y recopilar información más allá de las circunscripciones territoriales, información e indicios que eventualmente pueden utilizarse como elementos de convicción en un proceso penal. De esta forma, se torna en una técnica clave para enfrentar a la criminalidad digitalizada tal como es concebida en la actualidad.

[18] DELGADO, Joaquín. *Criminalidad Organizada*. Barcelona, España, J.M. Bosch, 2001, p. 24.
[19] POLITOFF, Sergio. *El agente encubierto y el informante infiltrado en el marco de la Ley 19.366 sobre tráfico ilícito de estupefacientes y sustancias sicotrópicas*. En: *Gaceta Jurídica*, N°203 Santiago, Chile, 1997, p. 8.

En este sentido, su mecanismo operativo consistiría en la infiltración de un agente policial en internet para que éste, esgrimiendo una identidad supuesta en su investigación, se gane la confianza, identifique y quite el velo del anonimato sobre los delincuentes digitales. Su mecanismo, naturalmente controversial, será basado en el engaño o fraude, procurando relacionarse de la manera más cercana posible con el investigado y vincularse a éste, siempre con el objeto de ingresar al mundo en que actúa y posibilitar la obtención de información necesaria en el marco de una investigación criminal.

La solución que nos entrega la figura del **agente encubierto informático** se encuentra en pleno auge legislativo a nivel internacional. Entendidos sobre la complejidad del escenario criminológico que se manifiesta en la "red de redes", es menester mirar qué puede decirnos al respecto el derecho comparado. En España, producto del clima europeo y en consonancia con la ratificación del *Convenio de Budapest*[20], la **Ley Orgánica 13/2015**, de 5 de octubre de 2015, introdujo a la Ley de Enjuiciamiento Criminal –de ahora en más "LECrim"– las prerrogativas necesarias para incorporar nuevas técnicas y formas de infiltración en el ordenamiento jurídico español, insertando formalmente la figura del agente encubierto informático. A continuación, en el Capítulo I, analizaremos su concepto, principales elementos, legislación, modo y ámbito de actuación, límites legales y los principales conflictos doctrinarios suscitados.

[20] Ratificado por España con fecha 1 de octubre de 2010.

CAPÍTULO I:

España y el agente encubierto informático

Dentro de las innovaciones más llamativas, útiles y controvertidas de la **Ley Orgánica 13/2015**, que con data de 5 de octubre de 2015, introdujo importantísimos cambios a la LECrim, encontramos precisamente la figura del **agente encubierto informático**. Como el concepto indica, la normativa regula el actuar de un agente policial encargado de investigar y descubrir eventuales delitos que sean cometidos en el ciberespacio. Cabe mencionar que el Tribunal Supremo de España, antes de la reforma, ya había reconocido la existencia de esta práctica policial[21], aunque sin tener presente sus consideraciones particulares, sino como una práctica propia de los agentes policiales en relación a su labor investigativa; como una práctica ordinaria del agente encubierto previamente regulado, algo similar a lo que sucede en nuestro país.

1. **Concepto**

En primer lugar, podemos definir al agente encubierto informático como "aquel empleado o funcionario público que, de manera voluntaria y por decisión de una autoridad judicial, se infiltra en la red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de ella, mediante la ocultación de su verdadera identidad policial y con el fin de establecer una relación de confianza que permita al agente integrarse durante un periodo de tiempo prolongado en el mundo en el que los ciberdelincuentes actúan, con la finalidad primordial e igualmente oculta, de obtener la información necesaria para desenmascarar a los supuestos criminales"[22].

De esta manera, podemos extraer los principales elementos que configuran esta herramienta investigativa:

a. Agente encubierto informático podrá ser todo **empleado** o **funcionario público**, entendido en la realidad española, y según establece la ley, como miembros de la **Policía Judicial**;
b. Exige **voluntariedad** en su actuar, debido a las implicancias morales que muchas veces pueden concurrir en el desarrollo de su labor. Asimismo, la LECrim en el apartado segundo del

[21] Tribunal Supremo, 3 de octubre de 2007, STS 767/07, España. En dicha causa, se logra condenar gracias a la utilización de un agente encubierto mediante internet, lo que es reconocido y validado en el fallo, que rechaza un recurso de casación y confirma la condena.
[22] BUENO DE MATA, Federico. "El Agente Encubierto en Internet: mentiras virtuales para alcanzar la justicia". En: *Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional)*, Coruña, España, 2011, p. 297.

artículo 282 bis estipula textualmente que ningún funcionario de la Policía Judicial puede ser obligado a actuar como agente encubierto;

c. Exigencia de **autorización judicial** por parte del **Juez de Instrucción** –siempre que se trate de canales cerrados de comunicación, como veremos– que se explica debido a la fuerte intromisión contra los derechos fundamentales que significa una medida basada en el engaño;
d. Su función será **infiltrarse en la red** con el propósito de **obtener y recabar información sobre partícipes** de determinadas conductas ilícitas que se desarrollen allí;
e. Su modo de actuar será mediante la **ocultación de su identidad** como policía y la utilización de una **identidad supuesta** o **ficticia**;
f. Deberá establecer una **relación de confianza** con los sujetos con quienes interactuará en la operación, fin primordial para que éstos le entreguen acceso a sus canales delictuales y a la información requerida para sacarlos a la luz.

A continuación, es menester analizar el articulado legal específico en que las características recién descritas encuentran asidero en la LECrim, con posterioridad a la reforma enunciada.

2. **Legislación**

La figura del agente encubierto "convencional", referida a infiltraciones en espacios físicos, se encuentra regulada en el **artículo 282 bis LECrim**, luego de una reforma en miras a perfeccionar las medidas investigativas relacionadas al delito de tráfico ilegal de drogas y otras actividades ilícitas graves, efectuada por la **Ley Orgánica 5/1999**, con data de 13 de enero de 1999.

Como ya fue anticipado, con la entrada en vigor de la **Ley Orgánica 13/2015**, en el referido artículo se añaden dos apartados más[23], los apartados 6 y 7, con la finalidad de introducir en la LECrim al **agente encubierto informático**, que tendrá como base las mismas condiciones fijadas para su antepasado, el agente encubierto "convencional".

Artículo 282 bis LECrim:

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

[23] Referidos a la nomenclatura y redacción de los cuerpos legales, los "apartados" en el derecho español vendrían a ser los equivalentes de los "numerales" en el derecho chileno.

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

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

3. **Procedencia**

La normativa establece como requisito fundamental de procedencia para el agente encubierto informático actuando en canales cerrados de comunicación, la existencia de una **autorización otorgada por el Juez de Instrucción**. Sobre este punto, concordamos con la tesis del "monopolio judicial"[24], entendiendo que la única figura competente para autorizar la utilización de esta herramienta investigativa –en canales cerrados de comunicación– será el Juez de Instrucción y no el Ministerio Fiscal dando cuenta inmediata al Juez, como es permitido en el proceder del agente encubierto "convencional".

Esta teoría encuentra su sustento principalmente en dos argumentos: (i) para establecer un mejor control sobre la medida, en el entendido de que permitir su utilización sin revisión judicial implica un aumento en el riesgo de afectar los derechos fundamentales de la ciudadanía, y (ii) un motivo netamente de texto, por cuanto el apartado sexto del artículo 282 bis LECrim establece literalmente que es la figura del Juez de Instrucción la que podrá autorizar a funcionarios de la Policía Judicial para que puedan desempeñarse como agente encubierto informático en canales cerrados de información, no mencionando en ningún momento al Ministerio Fiscal como sí lo hace el apartado primero, con su homólogo en espacios físicos.

Esta autorización deberá incluir el nombre real del funcionario de la Policía Judicial que oficiará como agente encubierto informático, así como el nombre e identidad falsa bajo la que desempeñará sus funciones, que le será otorgada por el Ministerio del Interior y que tendrá una validez de 6 meses, con opción de prórroga por el mismo período. Esta será la identidad supuesta que el agente utilizará a lo

[24] VELASCO NÚÑEZ, Eloy. Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías [en línea]. España: El Derecho, 2011. Disponible en: https://elderecho.com/novedades-tecnicas-de-investigacion-penal-vinculadas-a-las-nuevas-tecnologias [fecha de consulta: 27 de noviembre de 2020].

largo de su investigación, y que constará de datos personales básicos, puesto que no exige ser tan detallada como en el caso del agente encubierto en terreno[25].

En efecto, "la tarea del otorgamiento de identidad falsa quedaría reducido a trámites muy sencillos, nada equiparable con el agente encubierto que trabaja en el plano físico. No sería por tanto necesario crear un correcto mundo paralelo social creíble, por lo que el establecimiento de esta figura desde el punto de vista del coste económico no sería problemático, puesto que no supondría ningún desembolso de dinero para las arcas del Estado"[26].

Si observamos los pronunciamientos de la jurisprudencia en estas materias, podemos destacar el establecimiento de las prerrogativas que esta autorización judicial habilitante debe mencionar[27], y que además, corresponden a aspectos del agente encubierto informático que desglosaremos en su respectivo momento según avancemos en el presente capítulo:

1. Autorización del funcionario habilitado para poder intercambiar y enviar por sí mismo, en el periodo establecido, archivos ilícitos por razón de su contenido;
2. Mantener la resolución habilitante secreta y en pieza separada, que quedará en poder del Letrado de la Administración de Justicia;
3. Grabar íntegramente las conversaciones en el soporte correspondiente que se remitirá al juzgado donde constarán las grabaciones e imágenes con las transcripciones de interés;
4. En el caso de que la investigación pueda afectar a los derechos fundamentales, el agente deberá solicitar del organismo judicial competente las autorizaciones que establezca la Constitución y la ley;
5. Deberán adoptarse las debidas medidas de control para asegurarse que no se producirá ningún comportamiento por parte del agente que pueda constituir una provocación al delito, y;
6. Toda la información que obtenga el agente encubierto informático deberá ser puesta en conocimiento del juzgado a la mayor brevedad para valorar su conformidad con el artículo 282 bis de la LECrim.

El cuarto requisito enlistado coincide con lo señalado por el apartado tercero del artículo 282 bis LECrim, que indica de manera específica la necesidad de autorización judicial en particular, por parte del Juez de Instrucción, cuando durante la vigencia de actuación de agentes encubiertos, alguna de las labores o medidas de investigación que éstos deban tomar o ejecutar puedan generar afectaciones a los

[25] En el caso del agente encubierto "convencional", además de una identidad supuesta, se precisan muchos más detalles para que pueda efectuar su labor de manera segura y fehaciente, tales como una historia de vida, historial penal o policial, dirección propia, cuentas bancarias y públicas, líneas telefónicas o teléfonos celulares, etcétera.
[26] BUENO DE MATA, ob. cit., p. 302.
[27] Audiencia Nacional, 26 de abril de 2018, SAN 1519/18, España.

derechos fundamentales del investigado. Lo anterior, enfocado a nuestro tema de estudio, hemos de entenderlo en la hipótesis de que el agente encubierto informático necesite incurrir en alguna acción adicional para continuar con la investigación, lesiva de garantías constitucionales, pero que no sea de aquellas que le son típicas a su despliegue –como lo son el registro de las comunicaciones y el envío de archivos ilícitos por su contenido– que según enlistamos, le son concedidas en la autorización judicial habilitante de origen.

Por otro lado, también existen pronunciamientos en relación a las causas que motivan la autorización judicial de esta medida[28], a saber: (i) las posibles injerencias en derechos fundamentales amparadas en un engaño o simulación; (ii) la afectación de un derecho de nueva generación, como lo es la autodeterminación informativa[29], y; (iii) la necesidad de dotar al agente encubierto de "inmunidad", en sentido figurado, respecto de sus actuaciones, que objetivamente, podrían ser típicas y por ende, susceptibles de persecución penal.

Es importante señalar que esta autorización judicial no será requerida cuando el despliegue del agente encubierto informático se efectúe en canales abiertos de comunicación, lo que será desarrollado con mayor detalle en una sección posterior.

4. **Ámbito de aplicación**

En primer lugar, el artículo 282 bis LECrim establece, en su apartado primero, que el actuar del agente encubierto será procedente "cuando se trate de investigaciones que afecten a actividades propias de la **delincuencia organizada**".

Luego, en el apartado cuarto del mismo artículo, la ley nos entrega una definición de lo que debemos entender como "delincuencia organizada" para estos efectos, precisándola como "la **asociación de tres o más personas** para realizar, de **forma permanente o reiterada**, conductas que tengan como fin cometer alguno o algunos de los **delitos siguientes**" y enlista una serie de figuras delictivas, a saber:

a. Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal[30];
b. Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.
c. Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.

[28] Juzgado de lo Penal, 6 de julio de 2016, SJP 39/16, España.
[29] La "autodeterminación informativa" es el concepto que recibe aquel derecho fundamental derivado del derecho a la privacidad y que consiste en la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, o almacenados en medios informáticos.
[30] Todas las referencias de la presente sección deben ser entendidas al Código Penal español.

d. Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal.
e. Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.
f. Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal.
g. Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal.
h. Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal.
i. Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal.
j. Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal.
k. Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.
l. Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.
m. Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal.
n. Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal.
o. Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando.

Como podemos apreciar, el presente artículo consagra una lista taxativa o *númerus clausus* de figuras delictivas para hacer procedente el actuar del agente encubierto, que en principio, no permitirían su utilización en una investigación encubierta respecto de otras figuras penales existentes, incluso aquellas que también son materia de la criminalidad organizada, lo que suscita dificultades en la práctica[31].

[31] Antes de la reforma a la LECrim del año 2015, en España se discutía sobre la relevancia de modernizar las tácticas investigativas actuales, debido a la gran proliferación de comunidades cerradas de pederastas en la web. El problema se manifestaba a la hora de considerar si estas "comunidades" podrían ser consideradas "organizaciones criminales", con la finalidad de hacer procedente el actuar del agente encubierto tradicional. Fue el Tribunal Supremo de España, en STS 1444/04 con fecha 10 de diciembre de 2004, quien vino a dar una solución antes de la reforma comentada, al referirse a la naturaleza del concepto "delincuencia organizada" como agravante, estableciendo que "lo esencial en estos nuevos fenómenos delictivos está, precisamente, en que la simple utilización de la red de comunicaciones informáticas supone ya el aporte del elemento de coordinación y el empleo de medio excepcional que se proyecta hacia una mayor lesividad, imprescindibles, aunque no del todo suficientes, para la consideración de la existencia de una organización criminal". Años más tarde, mediante STS 767/07 con fecha 3 de octubre de 2007, el mismo tribunal, a modo complementario, nos señala que "el sólo hecho de difundir e intercambiar material pornográfico sugiere las intervención de dos o más personas". De esta forma, podíamos establecer que, previo a la reforma, el solo uso de internet como herramienta para la comisión del delito, al menos en aquellos cometidos por pederastas en canales cerrados, daba por cumplida la exigencia de "delincuencia organizada". Sin embargo, no podemos

Sin embargo, en el apartado sexto del mismo artículo, que como revisamos fue añadido por la Ley Orgánica 13/2015 e introdujo formalmente la figura del agente encubierto informático a la legislación española, se amplía este catálogo a tal punto, que es posible mitigar el requisito de "delincuencia organizada" establecido para la autorización y procedencia del agente encubierto convencional.

En efecto, la reforma en comento otorgó al agente encubierto informático la posibilidad de decretarse no solo para los delitos mencionados en el apartado cuarto del artículo 282 bis LECrim, sino además, para cualquiera de los previstos en el **artículo 588 ter a** del mismo cuerpo legal. Este articulado, asimismo añadido por la Ley Orgánica 13/2015, trata sobre los delitos que posibilitan la procedencia de interceptar comunicaciones telefónicas y telemáticas, y que de esta forma, amplían el espectro disponible para el actuar el agente encubierto informático. Estos son los siguientes:

a. Delitos contenidos en el artículo 579 apartado primero de la LECrim, que trata sobre la interceptación de la correspondencia escrita o telegráfica. En concreto, serían:
    a.1. Delitos dolosos castigados con pena límite máximo de, al menos, tres años de prisión;
    a.2. Delitos cometidos en el seno de un grupo u organización criminal;
    a.3. Delitos de terrorismo.
b. Delitos cometidos **a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación** o servicio de comunicación.

Esta última añadidura, que hace alusión a delitos cometidos a través de la utilización de cualquier tipo de TIC para su ejecución, permite expandir por completo el ámbito de procedencia del agente encubierto informático, sin requerir para su acción que se trate de actividades propias a la "delincuencia organizada".

Esta expansión de competencia para el agente encubierto informático actuando en comunidades cerradas de información es un asunto bastante controversial. Por un lado, permite la utilización de esta poderosa herramienta investigativa en muchas figuras penales que con anterioridad, no eran susceptibles de poder serlo, tales como el *childgrooming*[32] –que ya mencionamos anteriormente– o incluso algunos tipos penales netamente digitales, como el delito de ataque a sistemas informáticos[33]. Debemos tener presente que la gran variedad de tipos ilícitos existentes en la internet se nutren de manera permanente con la enorme cantidad de opciones que otorga la informática, evolucionando sus

omitir el hecho de que la figura del agente encubierto también es efectiva contra muchos otros delitos, más allá de los delitos cometidos por comunidades de pederastas. Finalmente, la reforma vino a eliminar estas dificultades conceptuales.

[32] Tipificado en España por la Ley Orgánica 5/2010, de 22 de junio de 2010. Artículos 183 y ss. Código Penal español.

[33] Tipificado desde un inicio en el texto original del Código Penal o Ley Orgánica 10/1995, actualizado por Ley Orgánica 5/2010 y Ley Orgánica 1/2015. Artículos 264 y ss. Código Penal español.

métodos día a día. Muchas de estas figuras no responden a la condición requerida en principio por la ley, es decir, que tengan un encaje en el concepto de "delincuencia organizada", sino que son efectuadas por personas de manera individual y en cualquier lugar del mundo, o a lo sumo, producto de la interacción con otros internautas, pero sin concierto previo ni organización alguna.

Por otro lado, y visto desde la perspectiva contraria, esta expansión implica mayor poder de control para el aparataje estatal, poder que eventualmente podría ser mal utilizado por la administración o las mismas fuerzas de orden, atentando directamente contra la privacidad y autonomía de los ciudadanos a pretexto de combatir el fenómeno del cibercrimen. Ante lo expuesto, podemos plantear que estos riesgos pueden disminuirse en la medida de que el examen de admisibilidad y proporcionalidad para la procedencia del agente encubierto informático, realizado por el Juez de Instrucción, sea lo suficientemente minucioso y meticuloso a la hora de analizar el tipo de delito que se quiere investigar, atendiendo al sentido común y a la gravedad del bien jurídico lesionado. Deberá constatar la existencia de indicios suficientes sobre la comisión del ilícito, que la medida sea idónea en su propósito y que sea realmente necesaria.

En conclusión, podemos afirmar que el agente encubierto informático es procedente para el siguiente listado de tipos delictuales:

a. Delitos contemplados en el artículo 282 bis apartado 4 LECrim, en el contexto de una organización criminal.
b. Delitos contemplados en el artículo 579 apartado 1 LECrim, a saber: (i) Delitos dolosos castigados con pena límite máximo de, al menos, tres años de prisión; (ii) Delitos cometidos en el seno de un grupo u organización criminal; (iii) Delitos de terrorismo.
c. Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

Existen autores que no comparten esta postura[34], esgrimiendo que todos los delitos a los cuales se ha expandido la competencia del agente encubierto informático, deben ser configurados entendiendo y tomando como base el requisito de la "delincuencia organizada", en el sentido que lo define la ley. Es decir, según esta postura, el agente en su faceta digital será procedente para el mismo listado de delitos que acabamos de establecer, pero siempre en el entendido que éstos sean cometidos por la asociación de tres o más personas y que éstos los ejecuten de forma permanente o reiterada.

[34] VALDIVIESO, Laura. *Las diligencias de investigación tecnológica y su aplicación práctica en el orden jurisdiccional penal*. Salamanca, España, TFM, Universidad de Salamanca, 2016, págs. 14-15.

Como ya aseveramos, entendemos que esta interpretación presenta inconvenientes prácticos, ya que muchas de las figuras delictivas que son cometidas mediante el uso de la red, escapan a estas características. Excluye de plano cualquier figura delictual que pueda ser desarrollada por una persona singular, algo que no es para nada extraño tal como hemos revisado a lo largo del presente trabajo, sobre todo considerando las amplias posibilidades y alto anonimato que otorga la internet. Además, si lo que se busca es poseer mayor control sobre esta medida investigativa, reiteramos que el enfoque debiese centrarse en el control de admisibilidad y proporcionalidad que realiza el Juez de Instrucción, chequeando la necesidad, idoneidad y adecuación de la medida, otra de las virtudes que presenta optar por el "monopolio judicial" a la hora de estimar la procedencia de esta herramienta de indagación.

Finalmente, reafirmamos que el actuar del agente encubierto informático será procedente, incluso cuando no se trate de "delincuencia organizada", en los siguientes delitos: (i) delitos dolosos con pena límite máximo de, al menos, tres años de prisión; (ii) delito de terrorismo y; (iii) delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación. Todo lo anterior, entendiendo la actuación del agente encubierto informático a través de canales de comunicación cerrados, puesto que en los canales de comunicación abiertos, la hipótesis cambia tal como revisaremos a continuación.

5. **Canales de actuación**

En base a lo enunciado, es posible distinguir dos grandes campos de actuación para el agente encubierto informático[35]: (i) actuación en canales o comunidades cerradas de comunicación, correspondiente al caso regulado por la LECrim, y; (ii) actuación en canales o comunidades abiertas de comunicación.

En primer lugar, la ley no nos entrega una definición para el concepto "canal de comunicación". Para efectos del estudio, definiremos este término como "todo medio físico o digital a través del cual se materializa un acto comunicativo, es decir, que sirve para el intercambio de información entre uno o varios emisores y uno o varios receptores". En este entendido, el acceso a dicho medio de comunicación, en nuestro caso digital, puede ser privado al público, como cualquiera de las aplicaciones de mensajería digital entre usuarios, o abierto, como las publicaciones en una red social.

[35] LAFONT NICUESA, Luis. "El agente encubierto en el Proyecto de Reforma de la LECrim". En: *Diario La Ley*, N°8580, España, 2015, p. 2.

5.1. Actuación en canales de comunicación cerrados

Esta corresponde a la hipótesis que introdujo la Ley Orgánica 13/2015 al artículo 282 bis LECrim, y que comprende la infiltración del agente encubierto informático en canales cerrados de comunicación, tales como aplicaciones de mensajería privada –como *WhatsApp*, *Telegram* o *Line*– así como mensajería privada en el contexto de una red social –como *Instagram* o *Facebook Messenger*–, servicios de correo electrónico –como *Gmail* u *Outlook*–, foros privados, comunidades por invitación insertas en la *dark web*[36], y un largo etcétera.

Los requisitos de procedencia para el agente encubierto informático actuando en canales cerrados de comunicación son los que hemos revisado hasta ahora en este trabajo, a saber: (i) exigencia de autorización judicial por parte del Juez de Instrucción; (ii) ser utilizado para la investigación de los delitos que estudiamos en la sección cuarta de este capítulo.

Es el actuar encubierto en el ámbito de canales cerrados los que le proporcionan una poderosa utilidad a esta herramienta investigativa, puesto que en muchos de éstos, no existe otra manera de poder penetrar o interceptar la información, en caso de ser requerido en el contexto de una investigación criminal. A modo de ejemplo, aplicaciones informáticas como WhatsApp, utilizan nuevas tecnologías de cifrado "de extremo a extremo", que hacen prácticamente imposible conocer el contenido de un determinado mensaje, imagen, audio o video, si no se es interlocutor en dicho intercambio de información[37].

5.2. Actuación en canales de comunicación abiertos

Por otro lado, encontramos un espectro de actuación diferente para el agente encubierto informático, aquel que se desarrolla en canales abiertos de comunicación. Nos referimos al también denominado "ciberpatrullaje", y que podemos definir como "aquella actuación policial destinada a la vigilancia, prevención y evitación de ilícitos en la red que tiene lugar en canales de comunicación abiertos, sin atentar contra el secreto de las comunicaciones, puesto que el acceso a la información contenida en estos canales puede efectuarlo cualquier usuario, no precisando autorización judicial para poder

[36] El concepto de "*dark web*" hace alusión a aquel contenido de internet que se encuentra oculto de las redes públicas y que requiere de aplicaciones, autorizaciones o configuraciones específicas para ser accesible. Se entiende inserto dentro del concepto de "*deep web*", que hace alusión a aquella fracción de internet que no se encuentra indexada por los motores de búsqueda.

[37] FAQ WhatsApp [en línea]. Disponible en: https://www.whatsapp.com/security/ [fecha de consulta: 30 de noviembre de 2020].

obtener lo que es público, más aún cuando el propio usuario de la red ha introducido voluntariamente dicha información en la misma"[38].

En este escenario de actuación, que ha tenido reconocimiento jurisprudencial previo a la reforma de la Ley Orgánica 13/2015[39], el agente encubierto informático **no requiere autorización judicial previa** debido a que no existe individualización ni identificación específica de algún sospechoso, ni se investiga algún delito en particular. Será el agente encubierto quien, por medio de un "*nickname*" o identidad ficticia –que tampoco requiere autorización judicial alguna[40]– podrá detectar acciones o elementos que existan de manera pública en internet y que puedan constituir figuras delictivas; pero siempre limitado a las herramientas al alcance de cualquier usuario de la web.

Lo afirmado también es tratado en la Exposición de Motivos de la Ley Orgánica 13/2015, donde además de describir algunos de sus atributos más característicos, se indica que la procedencia del agente encubierto informático "requiere autorización judicial para actuar en canales cerrados de comunicación, puesto que en los canales abiertos, por su propia naturaleza, no es necesaria"[41].

Con posterioridad a la reforma, también encontramos jurisprudencia que se ha manifestado respecto a este canal de actuación. En este sentido, con fecha 6 de julio de 2016, el Juzgado de lo Penal en Gijón aseveró que "en las actuaciones dirigidas a la vigilancia, prevención y evitación de ilícitos en las redes informáticas cuya evidencia tiene lugar en fuentes abiertas en la web o canales no cerrados de comunicación, se viene sosteniendo que la ocultación de la condición de agente de la policía haciéndose pasar por un usuario más en la red, en principio no requiere autorización judicial"[42].

6. **Herramientas de actuación**

En lo que respecta a las herramientas que la ley otorga al agente encubierto informático, con el propósito de que este las esgrima en su actuación en canales cerrados de comunicación y en apoyo a su labor investigativa, encontramos las siguientes: (i) la posibilidad de intercambiar archivos ilícitos por razón de su contenido; (ii) analizar los resultados de los "algoritmos" aplicados para la identificación

[38] TURIÑO, Paula. *La infiltración policial en el proceso penal: reforma de la Ley de Enjuiciamiento Criminal y el Agente Encubierto Informático*. Salamanca, España, TFM, Universidad de Salamanca, 2015, p. 37.
[39] Tribunal Supremo, 3 de octubre de 2007, STS 767/07, España. Refiriéndose al actuar de la policía, que mediante la técnica del "ciberpatrullaje" logró prevenir la ejecución de un posible delito de difusión de pornografía infantil, el Tribunal determina que éstos "realizaron las investigaciones oportunas y solo cuando tuvieron la convicción de estar efectivamente en presencia de hechos presuntamente delictivos, confeccionaron el oportuno atestado que remitieron a la Fiscalía (…) tal método de proceder es absolutamente correcto y ninguna objeción puede merecer".
[40] STS 767/07, ob. cit.
[41] Exposición de Motivos Ley Orgánica 13/2015, apartado IV parte final.
[42] SJP 39/16, ob. cit.

de dichos archivos ilícitos; (iii) la posibilidad de obtener imágenes y grabar conversaciones, y; (iv) la exención de responsabilidad criminal derivada del ejercicio de sus funciones.

6.1. Intercambio de archivos ilícitos

Para analizar esta medida, en primer lugar nos remitimos al apartado sexto que la reforma estudiada introdujo al artículo 282 bis LECrim, donde en su inciso segundo se contempla explícitamente la posibilidad de que el agente encubierto informático, previa autorización judicial específica para ello, intercambie o envíe por sí mismo archivos ilícitos "por razón de su contenido".

Esta herramienta a disposición del agente encubierto informático encuentra su justificación en miras de un mejoramiento respecto a su desarrollo y eficacia, ya que muchas de las comunidades cerradas de información que se encuentran en internet establecen trabas o requisitos para poder ingresar a ellas; ya sea la existencia de una invitación o referencia previa sobre el sujeto que busca ingresar, o bien el envío o aporte de determinado material "ilícito" que logre dar certezas y demuestre al agente como un igual frente al investigado[43].

Por su amplitud, esta posibilidad "puede abarcar cualquier tipo de investigación en torno a estos comportamientos en la red, desde intercambio de material pedófilo hasta intercambio de archivos protegidos por derechos de autor, distribuidos sin permiso de los titulares de dichos derechos"[44]. En efecto, lo anterior se ve reflejado en atención a comunidades de pederastas que "no se fían de la gente con la que hablan y piden algo con el fin de creer que están hablando con alguien con los mismos gustos que ellos"[45].

Es en este punto donde se suscita la primera controversia a analizar, y es que la ley española no nos ha entregado una definición de lo que debemos entender por "archivo ilícito". En nomenclatura textual de la ley, se hace referencia a "archivos ilícitos por razón de su contenido", por lo que entendiéndolo de manera amplia, aquella ilicitud puede manifestarse en dos facetas: (i) tanto en lo que dicho archivo puede realizar o ejecutar, como un virus *troyano* que recopile y envíe determinada información, o (ii) respecto del archivo enviado en sí mismo, desde un archivo *mp3* protegido por derechos de autor, hasta material pornográfico infantil. Respecto de la primera hipótesis no existe mayor debate, y es aceptado siempre que se cuente con la autorización judicial respectiva para aquello. Es dentro de la segunda

[43] La posibilidad de que el agente encubierto intercambie material ilícito con un individuo también se encuentra recogida en nuestra legislación, pero limitado al espectro de delitos relacionados a la pederastia o pornografía infantil, en el artículo 369 ter de nuestro Código Penal, tal y como revisaremos en la sección sexta del capítulo segundo.
[44] ROMERO, Pablo. El Gobierno quiere habilitar a policías para que puedan intercambiar "por sí mismos" archivos ilícitos en la red [en línea]. España: Diario El Mundo, 2014. Disponible en: https://www.elmundo.es/tecnologia/2014/12/05/54818e5cca4741c6218b4575.html [fecha de consulta: 2 de diciembre de 2020].
[45] BUENO DE MATA, ob. cit., p. 303.

hipótesis planteada, específicamente respecto del envío de material pornográfico infantil por parte del agente encubierto informático, en la que se ha manifestado mayor debate.

De interpretar que el material pornográfico infantil a disposición de ser enviado por el agente debe ser real, en el sentido de contener efectivamente menores de edad, solo quedaría la posibilidad de intercambiar material pornográfico existente, proveniente de antiguas investigaciones y que se encuentre debidamente resguardado por la institución competente, puesto que material de esta naturaleza no puede "fabricarse". Esta posibilidad otorgaría mayor veracidad a la coartada del agente, facilitando el desarrollo de la investigación, pero como desventaja, significaría volver a exponer a estos menores dentro de las redes pederastas. En esta misma línea de razonamiento, parte de la doctrina española ha manifestado que "se ha propuesto intercambiar material pornográfico de antiguas redadas, cuestión que no compartimos al defender siempre actuaciones que no impliquen a menores en todo el procedimiento, ya que creemos que por encima de toda investigación criminal, está la protección de la infancia"[46].

Por otro lado, siendo la postura a la que naturalmente adherimos, se contempla la posibilidad de prefabricar material pornográfico en que actores mayores de edad se hagan pasar por menores, o en los cuales exista intervención digital para crear la ilusión de que se trata de menores de edad. Esta medida se ubicaría en el límite de vulnerar aquello que paradójicamente se busca proteger, es decir, los valores y la imagen no corrompida de la infancia. "Pensamos aquí, que si existe una autorización judicial que lo permita, no estaríamos vulnerando la imagen de ningún menor ni de la infancia en su conjunto, debido a que sería material específicamente creado para luchar contra este fin –contra la producción y distribución de pornografía infantil– y en él no se estarían involucrando en ningún momento a personas menores de edad"[47].

En la misma dirección, se asevera que "podemos llegar a pensar que el texto normativo está permitiendo al agente el uso de material pornográfico real que hayan podido obtener en otras investigaciones pasadas. Ante esta idea, lo más lógico es pensar en material pornográfico simulado, o pseudo-pornografía artificial y virtual, de manera que bajo ninguna circunstancia entre los archivos intercambiados estén presenten menores de edad reales sino simulados mediante cualquier artificio que resulte útil"[48].

El principal conflicto que deviene de esta interpretación radicaría en que la producción de material pornográfico infantil fraudulento, sea mediante actores o mediante manipulación digital audiovisual,

[46] BUENO DE MATA, ob. cit., p. 303.
[47] BUENO DE MATA, ob. cit., p. 304.
[48] VALDIVIESO, ob. cit., p. 15.

tendría que mantener necesariamente relativa constancia, ya que se corre el riesgo de que dichos archivos se propaguen por internet con la información de que son falsos, o peor aún, con la información de que son utilizados por funcionarios policiales, perdiendo por completo su eventual eficacia en una investigación. De todas maneras, creemos que estos costos no son excesivos pensando en la protección de los menores y el resguardo de sus derechos.

Finalmente, debemos mencionar una última discusión suscitada a propósito del intercambio de material pornográfico infantil. Se ha planteado el conflicto de que la parte acusada solicite la nulidad del respectivo procedimiento, esgrimiendo que ha sido inducido por parte del agente encubierto informático a cometer el delito. La hipótesis del delito provocado se configuraría cuando el agente encubierto no limita su acción a las labores estrictamente investigativas, sino que influencia al investigado hasta incitarlo a delinquir, de manera tal que sin mediar aquella influencia, el delito no hubiese sido cometido.

Al respecto, la jurisprudencia ha establecido una doctrina muy consolidada en este respecto: "no cabe identificar ni confundir el "delito provocado" con el que ha venido en denominarse "delito comprobado", que tiene lugar cuando la actividad policial sin quebrar legalidad alguna, pretende descubrir delitos ya cometidos (…) toda vez que en estos supuestos el agente infiltrado no busca generar la comisión del delito, sino allegar las pruebas de una ilícita actividad ya cometida o que se está produciendo, pero de la que únicamente se abrigan sospechas. En el delito provocado no se da en el acusado una decisión libre y soberana de delinquir. En el delito comprobado esa decisión es libre y nace espontáneamente"[49].

Sobre esta controversia, nos decantamos por no identificar necesariamente el actuar del agente encubierto informático como la de un "agente provocador", puesto que esta hipótesis requiere que el agente induzca al investigado a cometer un delito que en principio no tenía intención de realizar, originando una voluntad criminal previamente inexistente. En el caso de la figura sujeta a estudio, existirá previamente una relación con el investigado, a fin de ganar su confianza y poder comprobar que con anterioridad, éste haya ejecutado conductas típicas afines a las investigadas. De esta forma, el envío de archivos por parte del agente encubierto informático no haría surgir en el investigado una voluntad criminal, puesto que esta existe con anterioridad a su intervención.

[49] Tribunal Supremo, 19 de febrero de 2003, STS 262/03, España.

6.2. Análisis de resultados algorítmicos en archivos ilícitos

El final del apartado sexto, en el artículo 282 bis LECrim, también contempla la posibilidad de que el agente encubierto informático analice los resultados de los algoritmos aplicados para la identificación de aquellos archivos ilícitos que puede intercambiar, según acabamos de estudiar.

Al respecto, las principales críticas han sido dirigidas hacia la redacción de lo que se quiere posibilitar, puesto que en concreto, el interés investigativo está en lo que se denomina código "*hash*", correspondiente a la clave alfanumérica que todo archivo digital posee y que es único en cada uno de ellos. La especificidad de esta clave alcanza tal nivel, que la más mínima alteración respecto del contenido o ubicación del archivo, logra modificarla.

El artículo 282 bis LECrim, al hablar de analizar el "resultado de los algoritmos", se está refiriendo precisamente a la posibilidad de que el agente encubierto informático analice el código "*hash*" de los archivos ilícitos que intercambia. En este sentido, la ley entiende el concepto de "algoritmo" como aquel procedimiento o serie de pasos necesarios para la obtención de un determinado resultado sobre un archivo, siendo aquel resultado en este caso, el código mencionado.

La importancia de este código viene a ser fundamental a la hora de poder rastrear los movimientos y modificaciones de los archivos ilícitos intercambiados por el agente encubierto informático, con el objeto de eventualmente destruirlos, así como poder diferenciarlos de otros archivos ilícitos que el investigado posiblemente maneje por cuenta propia, evitando confusiones e incriminaciones penales ilegítimas.

6.3. Grabación de imágenes y sonidos

En lo que respecta a la posibilidad de grabar imágenes y sonidos en conversaciones entre agente y sospechoso, nos remitimos al apartado séptimo del artículo 282 bis LECrim, añadido asimismo por la Ley Orgánica 13/2015. Este apartado establece que, durante el curso de una investigación y mediante autorización judicial habilitante, el agente encubierto podrá obtener imágenes y grabar conversaciones que mantenga en los encuentros previstos con el investigado, incluso cuando se desarrollen al interior de un domicilio.

Interpretando la norma en consonancia a la naturaleza del agente encubierto informático, ésta permitiría la captación de las conversaciones llevadas a cabo por este y el investigado en canales cerrados de comunicación. Tal sería el caso, a modo de ejemplo, de las capturas de pantalla en el caso de plataformas de mensajería privada, grabación de audios intercambiados por estas mismas

plataformas, o la captación de una llamada, online o mediante telefonía celular, en que el agente encubierto informático sea interlocutor.

Con todo, al ser un elemento tan directamente relacionado a la labor misma del agente encubierto informático, su autorización se realizará en conjunto con la autorización de procedencia del agente por parte del Juez de Instrucción; entendiendo que uno de los fines de esta medida investigativa ciertamente es recopilar antecedentes que comprueben la comisión de los delitos investigados, incluidas aquellas pruebas que atestigüen las conversaciones desarrolladas con el sospechoso. Así también lo considera la jurisprudencia[50], como ya mencionamos en la sección sobre procedencia de esta herramienta investigativa.

Debemos tener en consideración dos puntos: en primer lugar, cuando la grabación de imágenes y sonidos se realice en canales abiertos de comunicación no se requeriría habilitación judicial, debido a las cualidades del ciberpatrullaje ya estudiadas en el presente trabajo. En segundo lugar, la hipótesis estudiada es respecto de aquellas imágenes y sonidos que pueda captar el agente encubierto por sí mismo. Cuando es referido al equipo humano que apoya el despliegue del agente, que implica la intervención de otras personas, hablamos de una medida distinta, aunque regulada por la misma Ley Orgánica 13/2015, que introdujo el nuevo Capítulo VII en la LECrim, dentro del Título VIII del Libro II y que regula exclusivamente este punto.

6.4. Exención de responsabilidad criminal

El apartado quinto del artículo 282 bis LECrim, dispone una exención de responsabilidad penal para el agente encubierto designado legítimamente, que requiere la reunión de los siguientes requisitos: (i) que las acciones ejecutadas por el agente sean consecuencia necesaria de la investigación criminal; (ii) que aquellas actuaciones guarden la debida proporcionalidad con la finalidad de la investigación, y; (iii) que estas acciones no constituyan una provocación al delito.

Por otro lado, el agente encubierto informático sí deberá responder penalmente por aquellas actuaciones que no guarden relación con la investigación, que sean desproporcionadas en relación a sus fines, o cuando pretenda actuar de manera encubierta sin estar autorizado para ello.

Aunque el comienzo del apartado quinto del artículo 282 bis LECrim establece la norma de exención, en su inciso segundo se describe el procedimiento para exigir responsabilidad penal al agente encubierto. Con este propósito y según la ley, para poder proceder penalmente contra el agente por las actuaciones realizadas "a los fines de la investigación", pero que no cumplan con los requisitos

[50] SAN 1519/18, ob. cit.

enlistados para configurar la exención de responsabilidad, el respectivo Juez de Instrucción de la causa en que el agente actuó deberá, tan pronto tenga conocimiento de la actuación, requerir informe relativo a tal circunstancia de quien hubiere autorizado la identidad supuesta –que en el caso español, es el Ministerio del Interior– en atención al cual "resolverá lo que a su criterio proceda".

CAPÍTULO II:

Chile y el agente encubierto en línea

En lo respectivo a nuestro ordenamiento jurídico y a la figura del agente encubierto, se suscita un problema nada más al comenzar su estudio, y es que no se cuenta con una reglamentación armónica y sistemática que lo defina y establezca sus casos de procedencia, sino que por el contrario, se encuentra mencionado de forma dispersa en diversas leyes especiales que la han regulado en uno u otro sentido. Además, no existe legislación expresa respecto al despliegue del agente encubierto en escenarios digitales, más allá de meras menciones, lo que complejiza aún más el análisis desde la perspectiva del presente trabajo. Sin embargo, 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 nuestra legislación en miras del compromiso adquirido por Chile frente al Convenio de Budapest, se busca introducir formalmente a nuestro ordenamiento jurídico la figura del "**agente encubierto en línea**" –nomenclatura utilizada en dicho proyecto–, aunque acotada a un listado de delitos que este mismo establece. En el presente capítulo desglosaremos esta nueva herramienta investigativa, pendiente de aprobación según estas líneas son redactadas, analizando cada uno de sus elementos junto con anticiparnos a las controversias generadas por muchos de ellos en la legislación comparada.

1. **Concepto**

En primer lugar, debemos delimitar cómo es entendida la herramienta del agente encubierto "convencional" dentro de nuestro ordenamiento jurídico.

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"[51]. 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"[52].

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

[51] RIQUELME, Eduardo. "El agente encubierto en la ley de drogas. La lucha contra la droga en la sociedad del riesgo". En: *Revista Política Criminal*, N°2, Talca, Chile, Universidad de Talca, 2006, p. 17.
[52] POLITOFF, ob. cit., p. 8.

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 como estudiamos en el capítulo primero, 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.

Volviendo al objeto del presente trabajo y tomando en cuenta los elementos analizados hasta este punto, podemos definir la figura del agente encubierto en línea como aquel funcionario policial que, autorizado por el Juez de Garantía, a petición del Ministerio Público[53], 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[54] 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.

Asimismo, esta definición nos permite identificar los principales elementos de la herramienta objeto de estudio:

a. Agente encubierto en línea podrá ser todo **funcionario policial**, entendido en nuestro país como miembros de **Carabineros de Chile** y **Policía 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[55], siempre que la hipótesis sea desplegarlo en canales cerrados de comunicación;

[53] Nuestra legislación, en el artículo 257 del Código Procesal Penal, posibilita a los intervinientes de un procedimiento solicitar diligencias investigativas al fiscal, e inclusive, a pedir la reapertura de la investigación directamente al Juez de Garantía cuando dichas diligencias requeridas no fueron tomadas en consideración. Aunque en esta última hipótesis será el Juez quien ordene el cumplimiento de las diligencias, siempre será el Ministerio Público el encargado de solicitar las autorizaciones judiciales habilitantes respectivas, en caso de ser requeridas.

[54] La nomenclatura "*impedir*" es la misma que el proyecto boletín número 12192-5 utiliza al describir los objetivos del agente encubierto en línea, y debido a esto, es que la utilizamos a la hora de definirlo. Desde la perspectiva penal, *impedir* un delito podría significar que este nunca logre configurarse, ante lo cual, debemos entender que parte de los individuos afectados por la intervención de los agentes digitales, tendrán un menor o mayor grado de habitualidad en las conductas investigadas, lo que haría comprensible la utilización de dicho concepto. Por otro lado, quedaría por resolver si el eventual delito *impedido* pudiese configurar un delito frustrado o una tentativa de delito en los términos del artículo 7 del Código Penal.

[55] Artículo 9 CPP. Autorización judicial previa. Toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de autorización judicial previa.
En consecuencia, cuando una diligencia de investigación pudiere producir alguno de tales efectos, el fiscal deberá solicitar previamente autorización al juez de garantía.
Tratándose de casos urgentes, en que la inmediata autorización u orden judicial sea indispensable para el éxito de la diligencia, podrá ser solicitada y otorgada por cualquier medio idóneo al efecto, tales como teléfono, fax, correo electrónico u otro, sin perjuicio de la constancia posterior, en el registro correspondiente. No obstante lo anterior, en caso de una detención

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**[56];
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.

Sobre este último elemento, debemos comentar que en nuestra legislación 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.

Al no contar con una definición legal, la doctrina ha acudido a los autores más influyentes en el tema para poder elaborar una –atendiendo a su cualidad eximente–, entendiendo a la "obediencia debida" como "aquella institución de derecho penal eximente de la responsabilidad penal de un sujeto ante la comisión de una acción típica, por ser realizada ésta por un subordinado en virtud de una orden de un superior, previa relación jurídica entre ellos y un deber de obediencia establecido por el ordenamiento jurídico"[57]. Asimismo, una fracción de la doctrina nacional rechaza la denominación "obediencia

se deberá entregar por el funcionario policial que la practique una constancia de aquélla, con indicación del tribunal que la expidió, del delito que le sirve de fundamento y de la hora en que se emitió.

[56] Tal como revisamos en el capítulo primero, para el despliegue del agente encubierto en línea no existe necesidad de otorgar una nueva identidad desde el aparataje institucional, debido a que en el mundo de los internautas, la usanza de *nicknames* o apodos viene a ser la regla general. Este argumento también es utilizado para defender la práctica del "ciberpatrullaje". En caso de requerirse una nueva identidad "completa", producto de la naturaleza de la investigación, hemos de remitirnos al inciso tercero del artículo 25 de la Ley 20.000, que establece la obligación de materializarla a la Dirección Nacional del Servicio de Registro Civil e Identificación.

[57] RIVERO, Rocío. *Memoria: La Obediencia Debida de Órdenes Ilícitas en el Derecho Penal y Derecho Penal Militar Chileno y Español*. Valparaíso, Chile. Pontificia Universidad Católica de Valparaíso, 2016, p. 14.

debida", esgrimiendo que aquella involucra la idea de que el ordenamiento jurídico puede imponer un deber de acatar órdenes antijurídicas, lo que sería inadmisible, ya que lo prohibido no puede, al mismo tiempo, estar mandado[58]. Es por esto que optamos por el término "obediencia jerárquica".

Como tal, en nuestro derecho la "obediencia jerárquica" es una institución plenamente vigente, encontrándose recogida en distintos cuerpos legales: principalmente en los artículos 61 y 62 de la Ley 18.834, sobre Estatuto Administrativo, y en los artículos 159 y 226 del Código Penal. El análisis del articulado, así como los detalles sobre la naturaleza jurídica de esta institución exceden el propósito del presente trabajo.

En lo que nos atañe, hemos de señalar que las labores del agente encubierto se encuentran amparadas por el ordenamiento jurídico, y debido a esto, no podrían ser consideradas antijurídicas. Como en doctrina no existe controversia sobre la vigencia de la "obediencia jerárquica" para órdenes lícitas, esta es plenamente aplicable a la figura objeto del presente estudio, obligando a los funcionarios designados como agentes a acatar la designación, siempre que las órdenes que reciba se enmarquen dentro de las atribuciones que el derecho previamente les otorga. Por último y en consonancia a lo afirmado, podemos mencionar que según la doctrina nacional, en esta hipótesis sí podríamos hablar de "obediencia debida", puesto que al tratarse de una orden lícita nos encontramos al margen del derecho penal[59].

2. **Legislación**

Como ya fue anticipado, la figura del agente encubierto "convencional", referida a su actuar en espacios físicos, se encuentra regulada de forma dispersa a lo largo de nuestro ordenamiento jurídico. Dentro de las leyes más importantes que lo contemplan, se encuentra la **Ley 20.000** que 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". 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

[58] CURY, Enrique. *Derecho Penal, Parte General*. 2ª ed., Santiago, Chile, Editorial Jurídica, 1992, Tomo 2, p. 88.
[59] CURY, ob. cit., p. 89.

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 **12192-25**[60], 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.

No obstante, podemos señalar la hipótesis tratada por el artículo 369 ter de nuestro Código Penal, donde se regula el intercambio de material pornográfico infantil por agentes encubiertos, tales como fotos o videos –que estudiaremos más adelante–. 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. 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.

Artículo 12 Proyecto Boletín 12192-25:

Cuando la investigación de los delitos contemplados en los artículos 1°, 2°, 3°, 4°, 5° y 7° de esta ley lo hiciere imprescindible y existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en esta ley, el juez de garantía, a petición del Ministerio Público, quien deberá presentar informe previo detallado respecto de los hechos y la posible participación, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.

La orden que disponga la realización de estas técnicas deberá indicar circunstanciadamente el nombre y dirección del afectado por la medida y señalar el tipo y la duración de la misma, que no podrá exceder de sesenta días. El juez podrá prorrogar este plazo por un período de hasta igual

[60] Ingresado al Senado con fecha 25 de octubre de 2018, que busca establecer normas sobre delitos informáticos, derogar la Ley 19.223 y modificar otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.

duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en el inciso precedente.

De igual forma, cumpliéndose los requisitos establecidos en el inciso anterior[61]*, el juez de garantía, a petición del Ministerio Público, podrá ordenar a funcionarios policiales actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, con el fin de esclarecer los hechos tipificados como delitos en esta ley, establecer la identidad y participación de personas determinadas en la comisión de los mismos, impedirlos o comprobarlos. El referido agente encubierto en línea podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener también imágenes y grabaciones de las referidas comunicaciones. No obstará a la consumación de los delitos que se pesquisen el hecho de que hayan participado en su investigación agentes encubiertos. El agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.*

3. **Procedencia**

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, 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[62], haya

[61] 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**.

[62] Creemos que el proyecto de adecuación debiese requerir que el "informe detallado previo" sea entregado por el Ministerio Público de manera coetánea a la solicitud de despliegue del agente encubierto en línea, no solo por ser lo que dicta el sentido común, sino que además no se establece con qué plazo específico de anterioridad debe presentarse

presentado un "informe detallado" respecto de los hechos y la posible participación de los investigados.

Este camino abordado por el proyecto nos parece del todo adecuado, ya que elimina toda duda que puede suscitarse respecto de la necesidad de autorización y es congruente con entender lo intrusiva que puede llegar a ser la utilización del instrumento investigativo en estudio. Es en congruencia con esta idea, que el proyecto además dispone al Ministerio Público la obligación de presentar un informe detallado previo al Juez de Garantía, donde se relaten los hechos y los posibles vínculos que delaten la participación de los afectados por la medida, lo cual constituye una novedad que no encontramos presente en la legislación comparada estudiada.

En relación a este punto, podemos comentar que en nuestra legislación vigente, producto de la necesidad investigativa de utilizar agentes encubiertos que actúen en contextos informáticos y ante la falta de una regulación expresa, se entiende aplicable la normativa existente sobre el agente encubierto "convencional" a la hora de utilizarlo en su faceta "en línea". Esto nos plantea serios conflictos, ya que existen hipótesis en el derecho chileno en que el despliegue de agentes encubiertos "convencionales" no requiere de autorización judicial previa alguna, como revisaremos.

En efecto, tal es el caso de la Ley 19.974, que crea la Agencia Nacional de Inteligencia[63], y que en su artículo 31 otorga la facultad de disponer el empleo de agentes encubiertos directamente a los directores o jefes de los organismos de inteligencia, prescindiendo por completo de autorización judicial y al margen del Ministerio Público. Asimismo ocurre con la previamente mencionada Ley 20.000, que en su artículo 25, además de entregarnos la definición legal de esta figura, otorga al Ministerio Público de manera exclusiva la labor de autorizar el uso de agentes encubiertos, omitiendo por completo la necesidad de autorización judicial habilitante. Este último caso es más llamativo, debido a que dicha ley no limita la procedencia del agente a alguna lista taxativa de delitos[64], y además de permitirse en organizaciones delictuales, se amplía el concepto al de "meras asociaciones o agrupaciones con propósitos delictivos". Si bien este último punto podría considerarse favorable en lo que respecta a la figura sujeta a estudio –según hemos reiterado, muchos "ciberdelitos" no caben en la configuración de crimen organizado–, la falta de control judicial sobre la medida aumenta la

[63] Publicada en el Diario Oficial con fecha 2 de octubre de 2004. En su artículo 31, esta ley entrega a los directores o jefes de los organismos de inteligencia militar o policial, sin necesidad de autorización judicial, la discreción para disponer que alguno de sus funcionarios oculte su identidad oficial y se infiltre, con la finalidad de obtener información y recabar antecedentes, en organizaciones sospechosas de actividades criminales, siempre que se encuadre en actividades de *inteligencia* y *contra-inteligencia* que busquen resguardar la seguridad nacional del terrorismo, crimen organizado y narcotráfico.

[64] IVELIC MANCILLA, Alejandro. "El agente encubierto en los delitos de tráfico ilícito de estupefacientes". En: *Revista Jurídica del Ministerio Público*, N° 61, Santiago, Chile, Ministerio Público, 2014, p. 163.

posibilidad de que sea utilizada indiscriminadamente por los organismos policiales, afectando los derechos fundamentales de la ciudadanía.

Todo lo anterior debe entenderse en el contexto fijado por el artículo 9 del Código Procesal Penal, bajo el cual toda actuación del procedimiento que prive, restrinja o perturbe al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, requerirá de autorización judicial previa. Recordemos además que el mismo cuerpo legal, en su artículo 7, otorga la calidad de imputado a una persona desde la "primera actuación" del procedimiento dirigido en su contra, entendiendo como "primera actuación", cualquier diligencia o gestión, sea de investigación, de carácter cautelar o de otra especie, que se realizare por o ante tribunal con competencia criminal, el Ministerio Público –como en nuestra hipótesis– o la policía, en la que se atribuyere a una persona responsabilidad en un hecho punible.

Si somos rígidos en la interpretación, debemos entender que la sola designación de un agente encubierto, herramienta fundada en el engaño, ya implica una actuación dirigida contra el investigado que en algún grado "perturba" sus derechos fundamentales. Producto de esto y en consonancia con el citado artículo 9 del Código Procesal Penal, el investigado adquiere la calidad de imputado. Entendiendo entonces que la designación del agente es una medida intrusiva respecto del imputado, en todo caso debiese exigirse autorización judicial para desplegar la medida. Como sabemos, esto no es lo que sucede en la práctica, reservándose al Ministerio Público la facultad de autorizarla[65].

Por lo expuesto, reafirmamos nuestra postura de "monopolio judicial" a la hora de autorizar la procedencia del agente encubierto en línea, y el hecho de que el proyecto de adecuación lo regule de esta forma constituye una señal en la dirección adecuada. El mismo proyecto, tal como enumeramos en la presente sección, nos aclara el propósito de esta autorización judicial habilitante, precisamente verificar que el proceder de la medida sea "imprescindible y existieren fundadas sospechas en hechos determinados, de que una persona hubiese cometido o participado en la preparación o comisión de alguno de los delitos contemplados en esta ley". En esta misma línea se enmarca el requerimiento del "informe detallado previo" al Ministerio Público.

Tratándose de un proyecto de ley, no contamos con jurisprudencia que nos ayude a identificar los elementos que deberá contener la autorización del Juez de Garantía. Para poder enumerarlos, recurriremos a los requisitos establecidos en la normativa del proyecto de adecuación, auxiliándonos

[65] IVELIC MANCILLA, ob. cit., p. 154.

además con la Instrucción General[66] 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"[67] –ya que como revisamos se prescinde de habilitación judicial–, podemos extraer algunos de ellos para utilizarlos como guía en nuestro estudio. De esta forma, nos es posible establecer que la autorización judicial habilitante para el despliegue del agente encubierto en línea deberá contener:

1. "Nombre y dirección" del afectado o afectados por la medida investigativa;
2. Indicación del tipo de medida[68] 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[69];
3. Datos que permitan la individualización del agente encubierto y su nombre ficticio o clave bajo el cual se denominará;
4. Rol único de la causa en la cual será utilizado el agente encubierto, si es del caso;
5. Cuerpo policial al que pertenece el funcionario que oficiará de agente encubierto;
6. Medidas de protección para el agente que se estimen necesarias en cada caso;
7. 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;
8. Mención sobre la habilitación del agente para que éste obtenga imágenes y grabaciones de las comunicaciones que sostenga con el investigado.

Los primeros dos elementos se encuentran en el proyecto de adecuación, consagrados en el inciso segundo del artículo 12.

[66] 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.

[67] Técnicamente la Instrucción General citada aborda la designación de agentes encubiertos y agentes reveladores, siendo esta última la figura del funcionario policial que simula ser comprador o adquirente, para sí o para terceros, de sustancias estupefacientes o sicotrópicas, con el propósito de lograr la manifestación o incautación de la droga. He omitido mencionarlo debido a que no es parte del objeto del presente estudio.

[68] Debemos tener en consideración que el artículo 12 del proyecto de adecuación también hace aplicables las medidas investigativas de los artículos 222 a 226 del Código Procesal Penal, en relación a los delitos que regula.

[69] Queda por determinar si es necesario que el Ministerio Público, antes de solicitar la prórroga, vuelva a presentar el "informe previo detallado" respecto de los hechos y la posible participación de los investigados, requerido en el inciso primero del artículo 12 del proyecto de adecuación. Lo lógico es que no sea requerido una segunda vez, puesto que dicho informe ya fue presentado previo a la primera solicitud. Sería positivo que el proyecto lo aclarara para evitar conflictos de interpretación, ya que la normativa se remite a "los requisitos contenidos en el inciso precedente" de manera genérica para solicitar la prórroga de la medida, sin distinguir a cuales requisitos se refiere en particular.

Respecto del primer requisito, "nombre y dirección" del afectado por la medida investigativa, hemos de observar que producto de la naturaleza de las investigaciones en internet, existirán muchos casos en que no se tendrá un nombre concreto del sospechoso y mucho menos una dirección, datos que precisamente el accionar de un agente encubierto en línea puede revelar. De esta forma, aplicado a nuestra herramienta en estudio, consideramos que esta exigencia es totalmente inapropiada. El potente factor de anonimato en la red, mencionado en reiteradas ocasiones en el presente trabajo, genera que en la realidad, la mayoría del tiempo solo se cuente con un "*nickname*" o una página de perfil en alguna red social del sospechoso, muy lejos de su verdadero "nombre y dirección". Por otro lado, hemos de tener en consideración que este requisito fue añadido al proyecto en la última modificación que recibió[70], con fecha 29 de enero de 2021, donde se introdujo el segundo inciso del artículo 12. Hasta esta modificación, dicho requisito no existía para ninguna de las medidas investigativas que posibilita el proyecto. En conclusión, y teniendo presente además que este requisito tampoco se encuentra en la legislación comparada estudiada en el capítulo precedente, sería positivo que el proyecto de adecuación enmiende el camino y en definitiva, elimine este requisito para la procedencia del agente encubierto en línea.

El tercer elemento, relativo a la individualización nominativa del agente encubierto por parte del Ministerio Público, ha suscitado cierta controversia en nuestro país, puesto que existe jurisprudencia que no la exige directamente como requisito en la autorización de procedencia. En este sentido se ha manifestado la Segunda Sala de la Corte Suprema[71], confirmando a su vez una sentencia del Tribunal Oral en lo Penal de Concepción[72], aseverando que el inciso primero del artículo 25 de la Ley 20.000 no establece la obligación de que el Ministerio Público individualice al funcionario policial que vaya a oficiar como agente, sino solamente la obligación de autorizar la procedencia de la medida, correspondiendo a las policías su posterior designación específica, recurriendo a la historia fidedigna del establecimiento de la Ley 20.000 para justificar este cometido[73].

[70] Modificación hecha en segundo trámite constitucional de la Cámara de Diputados, con fecha 29 de enero de 2021.
[71] Corte Suprema, Segunda Sala, 22 de diciembre de 2016, Rol N° 87813/2016.
[72] Tribunal Oral en lo Penal de Concepción, 26 de octubre de 2016, RIT N° O-606-2016.
[73] Considerando undécimo de la sentencia de Corte Suprema en comento: "Que, en otro orden, y a diferencia de lo postulado en el arbitrio, el estudio de la historia fidedigna del establecimiento de la Ley N° 20.000 es concordante con lo que se viene razonando. En efecto, en el Mensaje Nº 232-341 de 2 de diciembre de 1999, con el que se inicia la tramitación de la ley que finalmente sustituye a la Ley N° 19.366, al definirse tanto al agente encubierto como al agente revelador, se expresa que ambos corresponden al 'funcionario policial *debidamente autorizado por sus superiores*' que realiza las actividades que luego describe. Pues bien, la supresión durante la tramitación del proyecto de la expresión '*debidamente autorizado por sus superiores*' tuvo por único objeto aclarar que tal permiso debe ser otorgado por el Ministerio Público y no por las policías, lo que se conforma con que aquel ente tiene la exclusividad en la dirección de la investigación, **pero sin con que con ello se buscase también que la nominación del funcionario que llevará adelante la diligencia sea efectuada por el Ministerio Público**. Es así como la indicación del Ejecutivo para eliminar la exigencia de anuencia del superior jerárquico policial se fundó en que en el nuevo sistema procesal penal, la única autoridad a la que le corresponde autorizar a este tipo de agentes es

En atención a esta controversia, nos inclinamos por la postura jurisprudencial, la que adecuándola a la naturaleza del agente encubierto en línea, entiende que no es obligatorio que el Juez de Garantía designe nominativamente a la persona que oficiará como agente encubierto. En el caso de la herramienta en estudio, la principal función de la autorización judicial viene a ser la de evaluar la procedencia de la medida, en atención a su proporcionalidad y los fines de la investigación, más no la de individualizar funcionarios policiales que por lo demás, usualmente el Juez desconocerá. Aquello, en línea con lo que expone la Corte Suprema, será labor del cuerpo policial correspondiente, que idealmente poseerá escuadrones especializados en este respecto[74].

Sobre las medidas de protección mencionadas en el sexto elemento, ante la ausencia de regulación por parte del proyecto de adecuación, debemos remitirnos a las establecidas en el artículo 30 de la Ley 20.000, para el agente encubierto "convencional", y solo en caso de ser posibles y razonablemente necesarias, ya que debido a la naturaleza de la actuación en espacios digitales, en la mayoría de las investigaciones podrá prescindirse de ellas.

Los últimos dos elementos enlistados, relativos al intercambio de archivos y la obtención de imágenes y grabaciones por parte del agente encubierto en línea, serán estudiados a mayor profundidad en la sección sexta del presente capítulo, referido a las herramientas que éste puede esgrimir en el ejercicio de sus labores de indagación.

4. **Ámbito de aplicación**

Como punto de partida, debemos entender que el proyecto de adecuación busca actualizar nuestra legislación en consideración al vertiginoso avance de las tecnologías. En el Mensaje, el ejecutivo hace hincapié en la necesidad de adoptar una nueva normativa a este respecto para Chile, que también incluya contenido de índole indagatorio, y constituya un pilar de lo que define como "Política Nacional de Ciberseguridad". Con este propósito, en el proyecto se establece un listado de delitos que se enmarcan en el ámbito de la cibernética, además de una serie de normas sustantivas entre las que se encuentra precisamente la figura del agente encubierto en línea.

Debido a lo expuesto, al menos hasta este punto, el 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

---

al Ministerio Público, ya que '**a la policía sólo le cabe designar al funcionario que desempeñará dicha función**' (Primer Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado)".

[74] Podemos agregar que, en relación a los mismos argumentos, tampoco estimamos necesaria la designación nominativa del agente encubierto en línea en la solicitud que de su procedencia debe realizar el Ministerio Público al Juez de Garantía.

adecuación, específicamente a los tipificados en los artículos 1º, 2º, 3º, 4º, 5º y 7º, consagrados en los preceptos que se indican[75]:

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;

Se excluye el delito de receptación de datos informáticos y el delito de abuso de dispositivos, establecidos en los artículos 6 y 8 del proyecto de adecuación respectivamente. Según apreciamos, se pretende establecer una lista taxativa de tipos penales en los cuales será procedente el despliegue del agente encubierto en línea, lo que, según analizamos en torno al derecho comparado en el capítulo precedente, presenta dificultades prácticas.

El problema que de forma particular se manifiesta en Chile, es que para aquellos tipos penales no considerados en el listado, que se encuadren normativamente dentro de la competencia de agentes encubiertos "convencionales" –como el regulado por la Ley 20.000– y que requieran el despliegue de agentes en internet, se seguirá prescindiendo de la revisión y autorización judicial correspondiente, ya que legalmente no es requerido. Este punto, además de implicar un aumento en el riesgo de afectación a los derechos fundamentales de la población, es incongruente con la esencia del agente encubierto en línea regulado en el proyecto, que de manera expresa establece la necesidad de autorización por parte del Juez de Garantía, generando falta de armonía legislativa en torno a una misma herramienta investigativa.

Como un aspecto positivo, en lo que respecta a la figura en estudio, debemos mencionar que el proyecto de adecuación **no establece la necesidad de una** "**organización delictual**" **o de** "**delincuencia organizada**" como requisito para permitir el accionar del agente encubierto en línea. Esto también es un acierto, ya que como estudiamos en el capítulo primero, un alto porcentaje del crimen cometido a través de internet prescinde completamente de aquellas características, bastando una sola persona para su completa ejecución. Además, de esta forma el proyecto también es consecuente

[75] Listado de delitos incluidos en el proyecto de adecuación actualizados al Segundo Trámite Constitucional de la Cámara de Diputados, con fecha 29 de enero de 2021.

con el catálogo de tipos penales que establece, todos susceptibles de ser llevados a cabo por un solo individuo.

Lo anterior, si bien puede significar polémico, creemos que es el camino adecuado, ya que tal como aseveramos en el capítulo anterior, si lo que se quiere es evitar que el aparataje estatal haga un eventual mal uso de esta herramienta investigativa, habrá que prestar atención a la revisión que el Juez de Garantía hará sobre la concurrencia de la medida. En efecto, mientras más meticuloso sea el Juez a la hora de evaluar lo "imprescindible" del despliegue del agente, su congruencia con los fines de la investigación, y de que existan sospechas fehacientemente fundadas contra los investigados sobre la comisión de los delitos, menor será el riesgo de afectación a los derechos fundamentales, evitando que se abuse de esta útil arma contra el crimen digital. Además, es en coherencia con esta idea que el proyecto de adecuación establece la obligación de presentar un informe detallado, por parte del Ministerio Público y previo a la solicitud de la medida, que incluya detalles sobre los hechos investigados y la posible participación del sospechoso.

Como último punto a mencionar respecto al ámbito de aplicación del agente encubierto en línea, creemos que establecer un catálogo *númerus clausus* de delitos no es lo óptimo, debido principalmente al vertiginoso progreso de las tecnologías, lo que en consecuencia, provoca una veloz evolución en los modos, formas y mecanismos a disposición del cibercrimen. En este mismo sentido se decantaba la doctrina española[76] al tratar esta controversia de forma previa a la reforma estudiada. Si bien es positivo que los tipos penales se encuentren descritos en armonía al Convenio de Budapest, esta cuestión encontraría una rápida solución si algún artículo del proyecto rompiera con la taxatividad del listado, aunque no lo hiciera para todas las medidas de investigación, que al menos fuera en concreto para el campo de actuación del agente encubierto en línea. A modo de ejemplo, podría extenderse a todos aquellos delitos perpetrados a través de las TIC o con ayuda de ellas, como en el caso español.

5. **Canales de actuación**

Tal como fue explicado en nuestra referencias sobre derecho comparado, es posible bifurcar el actuar del agente encubierto en línea principalmente en dos escenarios: (i) actuación en canales o comunidades cerradas de comunicación, correspondiente a la hipótesis regulada por el proyecto de adecuación, y; (ii) actuación en canales o comunidades abiertas de comunicación.

Nuestra legislación tampoco nos entrega una definición de lo que debemos entender por "canal de comunicación", por lo que nos remitiremos a la definición ya revisada en el capítulo primero,

[76] BUENO DE MATA, ob. cit., págs. 297-298.

entendiéndolo como "todo medio físico o digital a través del cual se materializa un acto comunicativo, es decir, que sirve para el intercambio de información entre uno o varios emisores y uno o varios receptores". Nuevamente, entenderemos que el acceso al "canal de comunicación" puede ser restringido al público o abierto a este.

5.1. Actuación en canales de comunicación cerrados

El proyecto de adecuación en estudio precisamente regula la hipótesis de infiltración del agente en canales cerrados de comunicación, puesto que como analizamos previamente, es en aquellos donde su accionar puede prestar la mayor utilidad dentro de los procedimientos investigativos, además de ser la que presenta mayores riesgos en cuanto a la afectación de derechos fundamentales.

Respecto de los requisitos de procedencia para el despliegue del agente encubierto en línea en canales cerrados, ellos son los mismos estudiados hasta este punto, a saber: (i) necesidad de autorización judicial por parte del Juez de Garantía, con todos sus requisitos de procedencia, y; (ii) ser utilizado para la investigación de alguno de los delitos establecidos en el proyecto de adecuación, detallados en la sección cuarta del presente capítulo.

Remitiéndonos a lo expuesto en la sección tercera, concordamos por completo con la exigencia de autorización judicial para el despliegue de esta herramienta en canales cerrados, puesto que es esta hipótesis la que habilita al agente encubierto en línea para ponerse en contacto con el investigado de manera directa, posibilidad delicada en relación al derecho a la inviolabilidad de las comunicaciones, establecido en el artículo 19 numeral 5 de nuestra Constitución Política de la República.

5.2. Actuación en canales de comunicación abiertos

En otro ámbito, y de la misma forma estudiada en el área internacional, en Chile podemos distinguir un segundo campo de actuación para el agente encubierto en línea; aquel que se desarrolla en canales abiertos de comunicación y que denominamos "ciberpatrullaje".

En la sección quinta del capítulo primero, definimos el concepto de "ciberpatrullaje" como "aquella actuación policial destinada a la vigilancia, prevención y evitación de ilícitos en la red que tiene lugar en canales de comunicación abiertos"[77] y que, en cuanto a nuestra legislación, no atenta contra el derecho a la inviolabilidad de toda forma de comunicación privada debido a que, por definición, el acceso la información contenida en un canal de comunicación abierto es público para cualquier persona, **sin necesidad de requerir autorización judicial habilitante**.

[77] TURIÑO, ob. cit., p. 37.

Este tipo de canal comunicativo hace referencia a aquella información contenida en perfiles o mensajes públicos que las mismas personas y de manera voluntaria suben a internet dentro del contexto de una red social, tales como *Facebook*, *Twitter* o *Instagram*. No infringe garantías constitucionales puesto que técnicamente no existe una interceptación de comunicaciones, además de no existir individualización previa de algún sospechoso o delito en concreto.

Esta práctica no es algo extraño en nuestro país, donde incluso existen unidades especializadas compuestas por grupos de informáticos, dentro de los respectivos cuerpos policiales, que buscan eventuales conductas delictuales en la web. Tal es el caso del Departamento OS-9 de Carabineros de Chile, destinado a la investigación de organizaciones criminales. En palabras de la teniente Javiera García, vocera del departamento el año 2018, "constantemente se mantienen monitoreos o patrullajes virtuales, revisando muchas redes sociales"[78]. Respecto de los funcionarios que componen estas unidades, afirma que "fueron capacitados por policías extranjeras", y que "no es que estén las 24 horas sentados" (frente al computador), sino que "aprovechan los beneficios de la tecnología portátil", efectuando el monitoreo también desde teléfonos celulares. En caso de detectar algún posible ilícito "el Ministerio Público es quien instruye qué va a pasar con la persona que logra ser ubicada"[79].

Finalmente, y en consonancia a la jurisprudencia estudiada en el capítulo primero, debemos agregar que el uso de "*nicknames*" o de identidades supuestas por parte de agentes en canales abiertos de internet tampoco debiese requerir autorización judicial habilitante, puesto que esta es la usanza común de los internautas y es parte de las posibilidades que dispone cualquier usuario de la web.

6. **Herramientas de actuación**

Corresponde ahora el estudio de las herramientas que el proyecto de adecuación ha otorgado al agente encubierto en línea en canales cerrados de comunicación con el propósito de auxiliar su labor investigativa, a saber: (i) intercambio o envío de archivos ilícitos por razón de su contenido; (ii) obtención de imágenes y grabaciones –material audiovisual– de las comunicaciones realizadas; (iii) particularidades en torno a la consumación del delito, y (iv) exención de responsabilidad penal derivada del ejercicio de sus funciones.

[78] RIVERA, Víctor. El desconocido "ciberpatrullaje" de Carabineros en las redes sociales [en línea]. Santiago, Chile: La Tercera Online, 28 de agosto de 2018. Disponible en: https://www.latercera.com/nacional/noticia/desconocido-ciberpatrullaje-carabineros-las-redes-sociales/299027/ [fecha de consulta: 4 de enero de 2021].
[79] Cómo funciona el "Ciberpatrullaje" que realiza Carabineros en redes sociales [en línea]. Santiago, Chile: Radio Cooperativa Online, 7 de septiembre de 2018. Disponible en: https://www.cooperativa.cl/noticias/pais/ff-aa-y-de-orden/carabineros/como-funciona-el-ciberpatrullaje-que-realiza-carabineros-en-redes/2018-09-07/183253.html/ [fecha de consulta: 4 de enero de 2021].

6.1. Intercambio de archivos ilícitos

La posibilidad de que el agente encubierto en línea intercambie archivos ilícitos en razón de su contenido se encuentra regulada en el mismo artículo 12 del proyecto de adecuación, dentro de su inciso tercero. Creemos, en atención a la experiencia española y según lo establecimos en la sección tercera del presente capítulo, que la posibilidad de intercambiar archivos ilícitos debe consagrarse en la autorización misma que el Juez de Garantía otorga sobre la procedencia del agente, por ser una cualidad fundamental en su labor investigativa, pero además por motivos de seguridad jurídica, evitando cualquier conflicto que pudiese derivar en la exclusión de prueba[80]. En este sentido, sería positivo que el proyecto de adecuación lo indicara como requisito específico de la autorización judicial habilitante, en vez de requerir otros que no vienen al caso, como el nombre y la "dirección" del investigado.

Como ha sido sostenido en el presente trabajo, el objetivo de entregar al agente esta opción encuentra su justificación en mejorar la eficacia de su despliegue, debido a la existencia de comunidades criminales cerradas en internet que establecen determinados requisitos de ingreso, entre ellos, el envío de determinado "material" que acredite la coartada del agente. Por otro lado, esta hipótesis también habilita al agente para enviar archivos ejecutables que, camuflados bajo la apariencia de cualquier otro tipo de archivo, recolecten y envíen de vuelta determinada información sobre el sospechoso.

Tal y como fue adelantado, la posibilidad de intercambio de archivos ilícitos mediante internet ya se encontraba en nuestra legislación, previo al proyecto de adecuación objeto de esta investigación. Sin embargo, al estudiarlo nos encontramos con ciertas complicaciones.

En primer lugar, el artículo 369 ter del Código Penal, añadido por la Ley 19.927[81], en su inciso segundo, establece que será procedente la intervención de agentes encubiertos en aquellos delitos relacionados a la prostitución de menores y a la producción y distribución de material pornográfico infantil[82]. Dispone como requisitos que su despliegue sea autorizado judicialmente, previa solicitud del Ministerio Público, que sea imprescindible en la investigación y que existan sospechas fundadas de que se están llevando a cabo delitos de la competencia del agente.

[80] Podría alegarse que la posibilidad de intercambiar archivos ilícitos no se entiende necesariamente concedida al agente encubierto en línea por la sola autorización de su procedencia. Luego, el agente encubierto no estaría autorizado para intercambiar archivos, y toda la prueba que pudo haberse obtenido de esta forma, deberá excluirse en un eventual procedimiento penal.

[81] Publicada en el Diario Oficial con fecha 14 de enero de 2004, que modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal en materia de delitos de pornografía infantil.

[82] Específicamente, para los delitos contemplados en los artículos 366 quinquies, 367, 367 ter, 374 bis inciso primero y 374 ter del Código Penal.

Hasta este punto todo claro, pero el inciso segundo del artículo 369 ter del Código Penal continúa, y añade que mediando igual autorización judicial, los organismos policiales pertinentes podrán mantener un registro reservado de "producciones del carácter investigado", con el objeto exclusivo de facilitar la labor de los agentes. Es aquí donde permite entregas vigiladas, en investigaciones donde se requiera el intercambio de dichas "producciones", en cualquier soporte. Para despejar dudas, el siguiente inciso nos aclara que "la actuación de los agentes encubiertos y las entregas vigiladas serán plenamente aplicables al caso en que la actuación de los agentes o el traslado o circulación de producciones se desarrolle a través de un sistema de telecomunicaciones". Aquí es donde se presentan inconvenientes.

Para empezar, se entrega la posibilidad de que los cuerpos policiales mantengan un registro de "producciones del carácter investigado", que no es otra cosa que un registro audiovisual de pornografía infantil. El problema es que la norma por sí sola no entrega mayores detalles[83] acerca del cómo debe conformarse este registro; exige autorización judicial habilitante pero, si el registro es uno, no se entiende si lo que requiere autorización judicial es la existencia misma del registro, o el hecho de que el agente encubierto requiera utilizarlo cuando sea necesario en la investigación –lo que nos parece más acertado–. Tampoco esclarece si es necesario que dichos registros sean reales, considerando que podrían ser "actuados" o alterados digitalmente, tal como analizamos en relación a esta misma posibilidad en el derecho comparado.

En esta línea de ideas, al desmenuzar los contenidos de la Ley 19.927, nos encontramos con que, además de añadir el artículo 369 ter a nuestro Código Penal, esta consagró un nuevo inciso al artículo 673 de nuestro viejo Código de Procedimiento Penal, que establece que "las producciones incautadas como pruebas de dichos delitos[84] podrán destinarse al registro reservado a que se refiere el inciso segundo del artículo 369 ter del Código Penal". Esta norma, en principio, vendría a solucionar la cuestión acerca de la procedencia de las "producciones" que la policía puede almacenar en Chile, estableciendo por ley que "podrá" componerse de prueba incautada en anteriores redadas, dejando de todas formas la posibilidad abierta y por ende, incierta.

Sobre este respecto, tal como planteamos en el capítulo anterior, no cabe más que manifestar rechazo, ya que con independencia de los fines que se esgriman, tal circunstancia vuelve a exponer a menores dentro de una red increíblemente nociva para su desarrollo como individuos. De esta forma, creemos

[83] Al estudiar la historia de la Ley 19.927, tampoco encontramos mayores especificaciones acerca del cómo debiese procederse respecto del registro de "producciones" a cargo de la policía, solo mencionando que se discutió si era o no necesaria autorización judicial.
[84] Refiriendo a los artículos 366 quinquies, 374 bis, inciso primero y 374 ter del Código Penal.

que el interés superior de todo niño, niña o adolescente[85] debiese primar, optando por soluciones como la de producir material pornográfico infantil "falso", que aunque implique costos producto de la frecuencia con que requiere ser artificiado, es congruente con la protección de la infancia. Con todo, la hipótesis de utilizar prueba de investigaciones pasadas quedó consagrada en el Código de Procedimiento Penal, que como sabemos, es de aplicación bastante restringida en la actualidad.

En consonancia a lo que hemos planteado, es menester citar la Instrucción General contenida en el Oficio 914/2015[86], que imparte criterios de actuación en lo referente a delitos sexuales, con data 17 de noviembre de 2015. Esta Instrucción establece interesantes tópicos en lo relativo al nombramiento de agentes encubiertos para tales delitos, como requerir un informe escrito y reservado a los fiscales, para sus respectivos superiores, donde establezcan el motivo o fundamento de la utilización de esta medida, o sugerir que su designación sea coetánea a las primeras actuaciones policiales, para legitimar su proceder y evitar futuras discusiones en torno a la licitud de su actuación. Pero en lo que nos compete, es que con respecto a las entregas vigiladas contempladas por el artículo 369 ter, la Instrucción es enfática en indicar que "los fiscales no deberán utilizar esta técnica cuando se trate de hacer circular material pornográfico infantil vía internet, debido a la dificultad de mantener una vigilancia efectiva del tráfico de éste, el que puede ser fácilmente difundido a otras personas, afectando los derechos de las víctimas y comprometiendo la responsabilidad del fiscal y de la policía".

De esta forma, la Instrucción prohíbe a los fiscales ordenar que los agentes encubiertos, en el contexto de actuación por delitos sexuales, realicen entregas vigiladas o intercambios de "producciones" a través de internet, principalmente para evitar que se difunda más aún y se continúen afectando los derechos de las víctimas. Esto, además de concordar nuestro punto, nos reafirma que la intención original de la ley efectivamente era la de utilizar "producciones" reales en el registro que mantendrían las policías. Ante todo lo expuesto, y ante la falta de una regulación acabada sobre este punto, que efectivamente se haga cargo de todas sus complejidades y particularidades[87], no podemos sino estar de acuerdo con la Instrucción General, que atiende al sentido común en cuanto a la protección de las víctimas.

Sin embargo, lo expuesto por la Instrucción General no soluciona qué hacer con la normativa del artículo 369 ter del Código Penal, que vista desde esta perspectiva se torna inútil, puesto que: (i)

[85] El interés superior de los niños, niñas o adolescentes es un principio rector que funda nuestro ordenamiento jurídico y está reconocido en el artículo 3 de la Convención de los Derechos del Niño. Significa que todas las decisiones que se tomen en relación a un niño, niña o adolescente deben ir orientadas a su bienestar y pleno ejercicio de derechos.
[86] Que reemplaza a la Instrucción General de Oficio 160/2009, con data 30 de marzo de 2009, relativa al mismo tema.
[87] La figura del agente encubierto en línea contenida en el proyecto de adecuación, si bien podría uniformar la regulación y solucionar los inciertos que hemos expuesto, de momento no es aplicable para esta clase de delitos. La solución para enmendar este rumbo, como hemos manifestado, es romper con la taxatividad de delitos que hacen procedente la herramienta en estudio.

concluimos que la composición del registro debía conformarse por "producciones" incautadas en investigaciones pasadas, pero la norma que lo habilita se encuentra en el antiguo Código de Procedimiento Penal, y; (ii) aunque igualmente pudiesen conformarse estos registros, finalmente no serían utilizados, por mandato expreso a los fiscales por dicha Instrucción.

Dicho lo anterior y retornando a la médula de este trabajo, como anticipamos al comienzo de la presente sección, el artículo 12 del proyecto de adecuación contempla específicamente para el agente encubierto en línea, la hipótesis de que éste intercambie por sí mismo "archivos ilícitos en razón de su contenido". Tal como en el caso de España, la legislación chilena no entrega una definición de lo que debemos entender por "archivos ilícitos en razón de su contenido", que además utiliza la misma nomenclatura ya estudiada. Producto de esto, de igual manera entenderemos que la ilicitud del archivo puede manifestarse en dos facetas: (i) ilicitud respecto de lo que el archivo eventualmente puede realizar o ejecutar, una vez alojado en el dispositivo del investigado, donde reiteramos el ejemplo de los clásicos virus *troyanos*, o (ii) ilicitud respecto del archivo en sí mismo, como las producciones audiovisuales de pornografía infantil o cualquier archivo protegido por derechos de autor o propiedad industrial.

Recordemos que el ámbito de actuación del agente encubierto en línea, tal como se encuentra regulado en el proyecto de adecuación, se limita a la lista de delitos que el mismo proyecto establece en el inciso primero del artículo 12, y que revisamos en la sección cuarta del presente capítulo. Entre ellos, no se encuentran mencionados los delitos relacionados a la producción y distribución de pornografía infantil, por ser un tema más allá de los objetivos del proyecto, y por tener estos una figura encubierta propia, como recién examinamos. Debido a esto, no corresponde aquí analizar más detalles de los mencionados respecto a esta clase de archivos ilícitos. Por otro lado, aquellos que serán útiles para los delitos informáticos contemplados en el proyecto, son los mencionados en la primera hipótesis analizada: archivos ilícitos respecto de lo que pueden ejecutar o realizar una vez alojados, de alguna manera, en los dispositivos informáticos de los investigados, con el propósito de revelar posibles pistas de la actividad igualmente ilícita de sus usuarios. Será el agente, por sí mismo, el encargado de efectuar los envíos de estos archivos, según lo habilita de manera expresa el proyecto de ley.

Finalmente, y en atención a las controversias analizadas, cabe agregar que en Chile no se contempla la posibilidad de que el agente analice los "resultados algorítmicos" en los archivos ilícitos que intercambie, como sí fue regulado en la legislación comparada estudiada en el capítulo primero. Esta posibilidad, que se vincula a las tecnologías de código "*hash*" revisadas anteriormente, en la práctica permite que el agente encubierto en línea tenga control sobre los archivos que intercambia con los investigados y los movimientos a los que aquellos sean sometidos. Creemos que sería positivo que el

proyecto de adecuación contemplara esta posibilidad, ya que prestaría mucha utilidad al desempeño del agente y sería del todo congruente con lo manifestado por el Ministerio Público en la Instrucción General sobre delitos sexuales revisada anteriormente, que si bien atiende a otra naturaleza de delitos, reconoce que existen problemas en relación a la vigilancia efectiva del tráfico del material intercambiado.

6.2. Grabación de imágenes y sonidos

El mismo artículo 12 del proyecto de adecuación consagra la posibilidad de que el agente encubierto en línea grabe imágenes y sonidos de las conversaciones que mantenga con el investigado, mediante cualquier dispositivo. En la práctica, esto se traduce en que el agente pueda tomar capturas de pantalla de los canales cerrados de comunicación mediante los cuales intercambie información con el sospechoso, así como grabar los "audios" o conversaciones en que el agente encubierto sea interlocutor.

Si bien no se encuentra exigido expresamente por el proyecto de adecuación, tal como sostuvimos en la sección tercera del presente capítulo, creemos que esta posibilidad para el agente debe quedar establecida en la misma autorización de procedencia por parte del Juez de Garantía, por ser una función que necesariamente requiere para desarrollar su investigación y porque, de esta manera, se evita cualquier discusión posterior acerca de la legitimidad de la prueba obtenida en uso de esta atribución. En relación a este punto, reiterando lo aludido sobre el intercambio de archivos ilícitos y por motivos de seguridad jurídica, sería positivo que el proyecto de adecuación requiriese de manera específica la mención de esta atribución en la autorización habilitante, eliminando toda controversia al respecto.

Cabe además recordar que, en caso de que la captación de imágenes o sonidos se realice en canales abiertos de comunicación, donde las personas de manera voluntaria realizan publicaciones de texto, imágenes o video, no es necesaria autorización judicial alguna.

6.3. Particularidades en torno a la consumación del delito

El proyecto de adecuación, en el mismo inciso tercero del artículo 12, se hace cargo de una de las principales polémicas estudiadas en la legislación comparada. La normativa dispone que "no obstará a la consumación de los delitos que se pesquisen el hecho de que hayan participado en su investigación agentes encubiertos". Esto debido a la problemática que podría suscitarse en caso que un imputado alegara no haber consumado por completo un determinado delito, arguyendo que el agente ejecutó una o varias fases de aquel. Este pasaje viene a eliminar toda controversia al respecto, indicando directa y claramente que de todas formas se podrá configurar la responsabilidad penal.

Cabe mencionar que hasta la reciente modificación que recibió el proyecto de adecuación, con fecha 29 de enero de 2021, el artículo 12 disponía que la intervención del agente encubierto en línea en una determinada investigación no sería considerada "inducción o instigación al delito". La motivación detrás de esta mención venía dada por las controversias suscitadas en este respecto a nivel internacional, que en parte estudiamos en la sección sexta del capítulo primero, analizando jurisprudencia española que distinguía entre los conceptos de "delito provocado" y "delito comprobado".

Lo que define al delito provocado, es que en él la voluntad de delinquir no nace directamente del investigado, sino que de alguna forma, la intervención del agente policial instiga a que aquella prolifere. En palabras de la Corte Suprema, para configurar la hipótesis de delito provocado en Chile, es necesario que el sospechoso sea objeto de "acoso, fuerza irresistible o miedo insuperable"[88] y que consecuencia de esto, ejecute el delito. Con determinada reserva, esta consideración normativa nos parecía positiva, siempre que ello no significara una "impunidad total" a priori para el agente. Finalmente, este pasaje fue eliminado del artículo, y con ello las controversias que podía suscitar. El debate acerca de considerar o no al agente como "instigador al delito" queda entregado a los tribunales competentes respecto de cada caso en particular.

6.4. Exención de responsabilidad criminal

La exención de responsabilidad criminal se contempla, de igual forma, a continuación del inciso tercero del artículo 12, en el proyecto de adecuación. Dispone que el agente encubierto en línea en sus actuaciones, estará exento de responsabilidad criminal "por aquellos delitos en que deba incurrir o que no haya podido impedir", siempre que (i) sean consecuencia necesaria del desarrollo de la investigación y (ii) guarden la debida proporcionalidad con la finalidad de la misma. La redacción de esta norma es la misma que encontramos en el anteriormente mencionado artículo 25 de la Ley 20.000, que regula la figura del agente encubierto "convencional" en nuestro sistema, y que en su último inciso, establece la exención de responsabilidad criminal para éste, en el mismo tenor utilizado por el proyecto de adecuación.

De la misma forma, entendemos a *contrario sensu* que el agente encubierto en línea podrá ser considerado responsable penalmente por aquellos delitos que haya podido impedir, por aquellos que no sean consecuencia necesaria de la investigación y por aquellos que no sean proporcionales con los fines de la investigación.

[88] Corte Suprema, Segunda Sala, 31 de octubre de 2001, Rol N° 801/2001, considerando 12°.

Finalmente, cabe mencionar que la exención de responsabilidad criminal fue incluida en las últimas modificaciones al proyecto de adecuación. Hasta dicha modificación no estaba considerada, lo que presentaba ciertas dificultades interpretativas[89] que de esta forma son superadas.

[89] Producto de los distintos delitos y requisitos de procedencia, una vez aprobado el proyecto, existirá en nuestra legislación una distinción entre la figura del agente encubierto "convencional" y la figura del agente encubierto en línea. Si el agente encubierto "convencional" posee exención contemplada de manera expresa, en el artículo 25 de la Ley 20.000, podía interpretarse que el agente encubierto en línea no tenía esa cualidad, ya que son dos figuras distintas.

EPÍLOGO

Los tiempos modernos han demostrado ser una vorágine sin precedentes en lo que respecta al progreso de las tecnologías, generándose una verdadera revolución digital desde la irrupción y posterior masificación de internet en el planeta, dando nacimiento a un nuevo mundo de interrelaciones e interacciones. Sin embargo, la infinidad de nuevas posibilidades que esto ha generado, tal como estudiamos en la presente investigación, ha posibilitado la aparición de complejos nuevos escenarios en el ámbito delictual.

En base a este planteamiento, creemos que un Estado de Derecho que aboga por la seguridad de sus ciudadanos, no debe quedarse simplemente observando el desarrollo del fenómeno informático, sino que debe hacerse partícipe de este y utilizarlo en su favor, siempre acorde a un marco legal determinado y con respeto a las garantías fundamentales. Según este contexto, la aparición de técnicas de investigación criminal tales como el agente encubierto en línea, vienen a significar un poderoso aliado en relación a figuras delictivas que hacen uso indiscriminado del alto grado de anonimato con que se puede operar en la "red de redes".

Ante el escenario internacional estudiado, nos parece de total atingencia que Chile realice una puesta al día en su legislación contra el crimen informático, además de responder a la obligación internacional contraída con la ratificación del Convenio de Budapest. El proyecto de adecuación es un paso en aquella dirección, sin embargo, en lo que respecta a la figura objeto de la presente investigación, se hacen necesarias ciertas precisiones que podrían mejorar la eficacia de su despliegue, así como el control que se puede tener sobre la misma y el respeto a los derechos fundamentales de las personas.

Tras el estudio y análisis del contexto legislativo chileno, así como de los detalles de la figura del agente encubierto en línea que busca ser insertada en aquel, podemos ultimar las siguientes ideas:

a. La figura del agente encubierto se encuentra regulada de manera dispersa y poco estructurada en nuestro ordenamiento jurídico, siendo lo más cercano a una regulación unitaria, aquella contenida en la Ley 20.000. Con la eventual añadidura de su vertiente digital, se suman motivos para establecer una normativa conjunta que, en congruencia con la importancia de esta herramienta investigativa y lo rigurosa que idealmente debiese ser su utilización, la regule y defina en un solo estatuto, todas sus atribuciones, limitaciones y ámbitos de actuación.

b. El requisito previo de “delincuencia organizada” o de “organizaciones criminales” es totalmente comprensible en el ámbito de procedencia del agente encubierto “convencional”, atendida la naturaleza de los delitos para los cuales originalmente fue pensado, pero no es congruente con la naturaleza de la delincuencia que se comete a través de internet. En este sentido, el hecho de que el proyecto de adecuación no exija estar en presencia de una “organización criminal” para permitir la utilización del agente encubierto en línea, nos parece la vía acertada en consideración a nuevas figuras delictuales que, haciendo uso de las TICs y los avances de las ciencias tecnológicas, pueden ser completamente ejecutadas por una persona de forma individual.

c. El requerimiento de autorización judicial para el despliegue del agente encubierto en línea, por parte del proyecto de adecuación, también nos parece una decisión correcta en miras de los peligros de afectación a los derechos fundamentales del investigado, además de coincidir con la tendencia en el derecho comparado. El control judicial de la medida permite un mayor monitoreo respecto a su procedencia, ya que el Juez de Garantía debe chequear que su uso sea imprescindible, existiendo además fundadas sospechas contra el investigado, basadas en hechos determinados, según versa el proyecto. En relación a lo expuesto en la letra b, la autorización habilitante también viene a mitigar el eventual uso excesivo que de la medida pudiesen hacer los organismos policiales, debido a la supresión de la “criminalidad organizada” como requisito para el actuar del agente.

d. Respecto de las enmiendas realizadas al artículo 12 del proyecto de adecuación, con fecha 29 de enero de 2021, el nuevo inciso segundo insertado dispone como requisito para la autorización judicial habilitante del despliegue del agente –o cualquiera otra de las medidas investigativas que el proyecto hace aplicables– que esta contenga el nombre y “dirección” del afectado por la medida. Tal como lo mencionamos en su momento, debemos hacer notar que producto del poderoso anonimato reinante en la red, la mayoría de las veces no existirá un nombre vinculado al sospechoso, y mucho menos una “dirección”, ya que estos datos son precisamente aquellos que el agente encubierto puede ayudar a revelar. En efecto, nos parece una exigencia completamente errada en miras de fortalecer la eficacia de nuestra herramienta en estudio, y esperamos que esto sea enmendado en un futuro. Finalmente debemos reiterar que este requisito tampoco es considerado en el derecho comparado estudiado en el capítulo primero.

e. La misma modificación del proyecto de adecuación mencionada en la letra d, introdujo un error en la redacción del artículo 12. Iniciando el inciso tercero, al enunciar la figura en estudio, el artículo 12 actual dispone: "De igual forma, cumpliéndose los requisitos establecidos en el *inciso anterior* (…)". Hasta esta última modificación, dicha referencia se entendía hecha al inciso primero del artículo 12, donde se establecen los delitos y los requisitos que hacen procedente el despliegue del agente encubierto en línea. Sin embargo, la modificación añadió un nuevo inciso segundo, donde también establece requisitos, por lo que el artículo debería referenciar a "los requisitos establecidos en los *incisos anteriores*", y no solo a los del "*inciso anterior*", de lo contrario nos quedaríamos sin los requisitos establecidos en el inciso primero del artículo 12, a saber: (i) imprescindibilidad de la medida, (ii) sospechas fundadas sobre el investigado, y (iii) la obligación de informe detallado previo a la solicitud para el Ministerio Público. Además, si no aplicamos el inciso primero del artículo 12, no se excluirían los delitos contenidos en los artículos 6 y 8 del proyecto para la procedencia del agente, en concreto, los delitos de receptación de datos informáticos y abuso de dispositivos. Esto, debido a la redacción del proyecto en el inciso tercero del artículo 12, que dispone al agente el fin de "esclarecer los hechos tipificados como delitos en esta ley", lo que incluye a todos los delitos que el proyecto tipifica, de no considerarse las exclusiones del inciso primero. Consideramos que la referencia a un solo inciso es un error del legislador, y esperamos que durante la tramitación restante del proyecto estos detalles puedan subsanarse, ya que pueden derivar en conflictos interpretativos innecesarios.

f. El listado taxativo de delitos en que podrá ser utilizado el agente encubierto en línea, establecido en el inciso primero del artículo 12 del proyecto de adecuación, también nos merece ciertas observaciones. En primer lugar, esta técnica legislativa es poco práctica en lo que respecta a la figura en estudio, puesto que el crimen informático evoluciona a la par y con la misma vigorosidad con que lo hace la tecnología. Un listado cerrado de tipos penales, por más detallado y elaborado que sea, está destinado a quedar obsoleto más temprano que tarde. La posible solución sería abrir la taxatividad de esta lista, autorizando el actuar el agente para todos aquellos delitos cometidos a través de instrumentos informáticos o de cualquier otra TIC, tal como lo estudiado en el derecho español. En segundo lugar, y particularmente en nuestro ordenamiento jurídico, con la eventual aprobación del agente encubierto en línea, existirá una diferencia entre éste y las demás figuras encubiertas de nuestra legislación, justamente producto de los distintos delitos de procedencia. El problema que se nos plantea, en relación a lo sostenido en la letra c, es que existen agentes encubiertos que no requieren de autorización

judicial, tal como estudiamos en la presente investigación, y esta situación generará una disparidad en nuestro derecho: mientras para los delitos contemplados en el proyecto, regirá la figura estudiada requiriendo de autorización judicial habilitante, para otros tipos de delitos, como aquellos que encuadren con la figura encubierta de la Ley 20.000, se seguirá prescindiendo del control judicial de la medida, incluso aunque esta se vea extrapolada a un contexto informático. Si legislaremos sobre agentes encubiertos en la red, sería positiva la existencia de una normativa armónica que regulara en un solo estatuto y de manera clara aquellas hipótesis en que podrán utilizarse, así como establecer la necesidad, en todo caso, de autorización judicial habilitante para su designación, debido a las fuertes implicancias vulneratorias de garantías constitucionales que envuelve investigar personas en canales cerrados de comunicación.

g. El "ciberpatrullaje", consistente en el monitoreo y fiscalización que agentes policiales realizan en canales abiertos de comunicación en internet, si bien puede ser considerada una medida polémica, se encuentra en completa consonancia con el catálogo de derechos fundamentales de nuestra Constitución, además de ser contemplada en el derecho comparado. Como efecto colateral y producto de la vigilancia, podríamos decir que esta circunstancia, al menos en algún grado, ayuda a fomentar la responsabilidad digital con que las personas actúan en canales abiertos de comunicación.

h. La hipótesis de intercambio por parte del agente, de archivos ilícitos en razón de su contenido, regulada por el proyecto de adecuación, también hace necesaria ciertas observaciones. El conflicto dice relación con la normativa vigente, pues como analizamos, el artículo 369 ter del Código Penal ya contemplaba la posibilidad de entregas vigiladas "a través de un sistema de telecomunicaciones", pero limitado a aquellos delitos relacionados a la producción y distribución de pornografía infantil. El problema, como fue estudiado en detalle, se materializa en que aquella norma se torna inútil, ya que por orden expresa del Ministerio Público se prohibió su utilización a los fiscales, y en segundo lugar, nunca se entregaron mayores detalles respecto de la medida en sí misma. Ante la añadidura de la posibilidad de intercambiar archivos ilícitos para el agente encubierto en línea, limitada a su espectro de delitos, y en relación a lo expuesto en la letra f, se hace aún más imperiosa la necesidad de una normativa uniforme que regule de manera acabada todas las hipótesis penales en que el agente digital puede intercambiar archivos, y también, específicamente qué clase de archivos puede intercambiar, en atención a la ley vigente del art. 369 ter del Código Penal y la efectiva protección de los niños, niñas y adolescentes.

i. En relación a lo anterior, la Instrucción General que imparte criterios de actuación en delitos sexuales para los fiscales, reconoce explícitamente que existen problemas de vigilancia sobre el tráfico de los archivos que eventualmente pudiesen intercambiarse. Ante dicho conflicto, creemos que sería útil entregar atribuciones al agente que ayuden a mantener un monitoreo efectivo sobre estos archivos. La solución estudiada en la legislación comparada dice que relación con la posibilidad de que el agente analice "los resultados algorítmicos" de los archivos ilícitos que intercambia, lo que en la práctica se traduce en el control del mismo sobre el código "*hash*", herramienta que en palabras sencillas, permite conocer todos los movimientos a los que ha sido sometido un determinado fichero. Esto facilitaría la vigilancia y rastreo sobre los archivos enviados, permitiendo su diferenciación de otros que pudiesen ser similares y eventualmente, su destrucción.

j. Finalmente, creemos que la introducción del agente encubierto en línea por medio del proyecto de adecuación, significa un positivo primer paso para nuestro país considerando los vastos avances del mundo del crimen en internet, sin embargo, producto de las limitaciones en sus requisitos de procedencia, su ámbito de actuación se verá reducido solo a aquellos tipos penales designados. Debemos tener en consideración que con el avance del tiempo, y la consecuencial migración de todo tipo de actividades antes cotidianas, al mundo informático, el uso de herramientas de indagación como la estudiada no harán más que aumentar su importancia investigativa, por lo que creemos que establecer límites formales en cuanto a los tipos penales, no se condice con su propia naturaleza. Creemos que una medida tan importante para los tiempos modernos, como lo es el agente encubierto en línea, idealmente merece su propia regulación individual y acabada; teniendo en mente tanto la ayuda que puede prestar dentro de los cuerpos policiales de investigación, como la protección a las garantías constitucionales de la ciudadanía usuaria del ciberespacio.

BIBLIOGRAFÍA CONSULTADA

LIBROS, ARTÍCULOS Y ENSAYOS:

1. ÁLVAREZ, Luis. Así funciona la ciberdelincuencia, el negocio ilícito más lucrativo [en línea]. Madrid, España: El Mundo, 2017. Disponible en: https://www.elmundo.es/economia/2017/01/08/586fc1d222601d6f4b8b4584.html [fecha de consulta: 12 de noviembre de 2020].

2. BUENO DE MATA, Federico. "El Agente Encubierto en Internet: mentiras virtuales para alcanzar la justicia". En: Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional), Coruña, España, 2011.

3. CARRIZO, Emiliano. El consumo de internet se dispara en Chile [en línea]. Santiago, Chile: La Tercera Online, 5 de octubre de 2020. Disponible en: https://www.latercera.com/pulso/noticia/consumo-de-internet-sube-durante-este-primer-semestre-y-el-uso-de-datos-para-jugar-se-dispara-mas-del-100/ [fecha de consulta: 10 de noviembre de 2020].

4. CASTELLS, Manuel. La sociedad red: una visión global. Madrid, España, Alianza Editorial, 2006.

5. Cómo funciona el "Ciberpatrullaje" que realiza Carabineros en redes sociales [en línea]. Santiago, Chile: Radio Cooperativa Online, 7 de septiembre de 2018. Disponible en: https://www.cooperativa.cl/noticias/pais/ff-aa-y-de-orden/carabineros/como-funciona-el-ciberpatrullaje-que-realiza-carabineros-en-redes/2018-09-07/183253.html/ [fecha de consulta: 4 de enero de 2021].

6. CURY, Enrique. Derecho Penal, Parte General. 2ª ed., Santiago, Chile, Editorial Jurídica, 1992, Tomo 2.

7. DELGADO, Joaquín. Criminalidad Organizada. Barcelona, España, J.M. Bosch, 2001.

8. Exposición de Motivos Ley Orgánica 13/2015.

9. FAQ WhatsApp [en línea]. Disponible en: https://www.whatsapp.com/security/ [fecha de consulta: 30 de noviembre de 2020].

10. HERRERA, Myriam. “El fraude informático. Actualidad penal”. En: Actualidad penal, N°39, España, 2001.

11. IVELIC MANCILLA, Alejandro. “El agente encubierto en los delitos de tráfico ilícito de estupefacientes”. En: Revista Jurídica del Ministerio Público, N° 61, Santiago, Chile, Ministerio Público, 2014.

12. KEMP, Simon. Digital 2019: Global internet use accelerates [en línea]. WeAreSocial.com, 30 de enero de 2019. Disponible en: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates/ [fecha de consulta: 10 de noviembre de 2020].

13. LAFONT NICUESA, Luis. “El agente encubierto en el Proyecto de Reforma de la LECrim”. En: Diario La Ley, N°8580, España, 2015.

14. MENDÍA, Rosario. “Delincuentes de la web: La pandemia como escenario favorable”. En: La Tercera, Santiago, Chile, 16 de mayo de 2020.

15. MITCHSONI / URRY. “Delitos y abusos en el comercio electrónico”. En: The IPTS Report, Centro Común de Investigación de la Comunidad Europea, 2001.

16. PLACENCIA, Felipe. Carabineros de Concepción captura banda que vendía con método “delivery” [en línea]. Concepción, Chile: Diario Concepción, 2020. Disponible en: https://www.diarioconcepcion.cl/ciudad/2020/07/08/carabineros-de-concepcion-captura-banda-que-vendia-droga-con-metodo-delivery.html [fecha de consulta: 9 de septiembre de 2020].

17. POLITOFF, Sergio. El agente encubierto y el informante infiltrado en el marco de la Ley 19.366 sobre tráfico ilícito de estupefacientes y sustancias sicotrópicas. En: Gaceta Jurídica, N°203 Santiago, Chile, 1997.

18. Reporte Explicativo del Convenio sobre Ciberdelincuencia del Consejo de Europa, párrafo 16.

19. REYNA, Luis. “La víctima en el delito informático”. En: Revista peruana de doctrina y jurisprudencia penal, N°1, Lima, Perú, 2002.

20. RIQUELME, Eduardo. “El agente encubierto en la ley de drogas. La lucha contra la droga en la sociedad del riesgo”. En: Revista Política Criminal, N°2, Talca, Chile, Universidad de Talca, 2006.

21. RIVERA, Víctor. El desconocido “ciberpatrullaje” de Carabineros en las redes sociales [en línea]. Santiago, Chile: La Tercera Online, 28 de agosto de 2018. Disponible en: https://www.latercera.com/nacional/noticia/desconocido-ciberpatrullaje-carabineros-las-redes-sociales/299027/ [fecha de consulta: 4 de enero de 2021].

22. RIVERO, Rocío. Memoria: La Obediencia Debida de Órdenes Ilícitas en el Derecho Penal y Derecho Penal Militar Chileno y Español. Valparaíso, Chile. Pontificia Universidad Católica de Valparaíso, 2016.

23. ROJAS, Elisabeth. Entrevista a Silvia Barrera, Jefa de la Sección Técnica del Grupo de Investigación en Redes de la Unidad de Investigación Tecnológica (UIT) del Cuerpo Nacional de Policía [en línea]. España: McPro, 2017. Disponible en: https://www.muycomputerpro.com/2017/03/17/silvia-barrera-cnp [fecha de consulta: 13 de noviembre de 2020].

24. ROMERO, Pablo. El Gobierno quiere habilitar a policías para que puedan intercambiar “por sí mismos” archivos ilícitos en la red [en línea]. España: Diario El Mundo, 2014. Disponible en: https://www.elmundo.es/tecnologia/2014/12/05/54818e5cca4741c6218b4575.html [fecha de consulta: 2 de diciembre de 2020].

25. Subsecretaría de Telecomunicaciones de Chile [en línea]. Santiago, Chile: Página web Subsecretaría de Comunicaciones, 2020. Disponible en: https://www.subtel.gob.cl/trafico-total-de-internet-fija-y-movil-crece-40-a-marzo-de-2020-impulsado-por-la-pandemia-de-covid-19/ [fecha de consulta: 9 de septiembre de 2020].

26. TURIÑO, Paula. La infiltración policial en el proceso penal: reforma de la Ley de Enjuiciamiento Criminal y el Agente Encubierto Informático. Salamanca, España, TFM, Universidad de Salamanca, 2015.

27. VALDIVIESO, Laura. Las diligencias de investigación tecnológica y su aplicación práctica en el orden jurisdiccional penal. Salamanca, España, TFM, Universidad de Salamanca, 2016.

28. VELASCO NÚÑEZ, Eloy. Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías [en línea]. España: El Derecho, 2011. Disponible en: https://elderecho.com/novedades-tecnicas-de-investigacion-penal-vinculadas-a-las-nuevas-tecnologias [fecha de consulta: 27 de noviembre de 2020].

29. VELASCO, Cristos. La jurisprudencia y competencia sobre delitos cometidos a través de cómputo e internet. 1ª ed., España, Tirant Lo Blanch, 2012.

30. VILLARROEL, María José. Detienen a acusado de realizar "delivery" de droga [en línea]. Santiago, Chile: Radio Bio Bio, 2020. Disponible en: https://www.biobiochile.cl/noticias/nacional/region-metropolitana/2020/07/09/detienen-acusado-realizar-delivery-droga-intento-atropellar-pdi-fiscalizacion-rm.shtml [fecha de consulta: 9 de septiembre de 2020].

JURISPRUDENCIA CHILENA:

31. Corte Suprema, Segunda Sala, 31 de octubre de 2001, Rol N° 801/2001.

32. Corte Suprema, Segunda Sala, 22 de diciembre de 2016, Rol N° 87813/2016.

33. Tribunal Oral en lo Penal de Concepción, 26 de octubre de 2016, RIT N° O-606-2016.

JURISPRUDENCIA ESPAÑOLA:

34. Audiencia Nacional, 26 de abril de 2018, SAN 1519/18.

35. Juzgado de lo Penal, 6 de julio de 2016, SJP 39/16.

36. Tribunal Supremo, 19 de febrero de 2003, STS 262/03.

37. Tribunal Supremo, 3 de octubre de 2007, STS 767/07.