



**VNIVERSIDAD
D SALAMANCA**

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO FIN DE GRADO

GRADO EN DERECHO

**Departamento de Derecho Administrativo, Financiero y
Procesal**

Derecho Procesal

Curso 2021/2022

El agente encubierto informático: Especial referencia a su actuación en los delitos de grooming y relativos a la pornografía infantil

Nombre del estudiante: Rubén González de Castro

Tutor: Dr. D. Federico Bueno de Mata

Junio de 2022

TRABAJO FIN DE GRADO

GRADO EN DERECHO

**Departamento de Derecho Administrativo, Financiero y
Procesal**

Derecho Procesal

**El agente encubierto informático:
Especial referencia a su actuación en los
delitos de grooming y relativos a la
pornografía infantil**

**The computer undercover agent:
Special reference to his performance in
the crimes of grooming and related to
child pornography**

**Nombre del estudiante: Rubén González de Castro
e-mail del estudiante: rubengdc00@usal.es**

Tutor: Dr. D. Federico Bueno de Mata

RESUMEN

El agente encubierto y el agente encubierto informático son figuras recientes en el ordenamiento jurídico español, empleadas como diligencias de investigación en procesos penales de criminalidad organizada y de delitos realizados por medio de Internet, en los que no cabe otra medida que permita obtener piezas de convicción acerca del hecho delictivo. Su designación bajo identidad supuesta, sus actuaciones en la infiltración regidas por una serie de límites y garantías y su presencia posterior en el juicio oral serán tratadas en el trabajo, sobre todo en atención a la medida más reciente referida al agente encubierto informático. De esta manera, podremos comprobar la absoluta necesidad de una diligencia como esta en nuestra normativa procesal penal ante la realidad, continuamente cambiante, de la tecnología a la que, rápidamente, se adaptan los delincuentes. Para ello, contemplaremos específicamente la actuación del agente encubierto informático en delitos cometidos sobre menores como son el grooming y aquellos relativos a la pornografía infantil. Con ello, podremos confirmar, con absoluta evidencia, que el Derecho debe evolucionar según las circunstancias lo requieran para atajar los sucesivos y novedosos comportamientos delictivos.

PALABRAS CLAVE

Agente encubierto, agente encubierto informático, *grooming*, *sexting*, pornografía infantil.

ABSTRACT

The undercover agent and the computer undercover agent are recent figures in the Spanish legal system, used as investigative procedures in criminal proceedings of organized crime and crimes carried out through the Internet. In both of them, there is no other measure that allows obtaining pieces of conviction about the criminal act. His designation under assumed identity, his actions in the infiltration governed by a series of limits and guarantees and his subsequent presence in the oral trial will be treated in the project, especially in attention to the most recent measure referred to the computer undercover agent. In this way, we will be able to verify the absolute need for a diligence like this in our criminal procedural regulations in the face of the constantly changing reality of the technology to which criminals quickly adapt. For this, we will specifically contemplate the performance of the undercover computer agent in crimes committed against minors, such as grooming and those related to child pornography. With this, we will be able to confirm, with absolute evidence, that the Law must evolve as the circumstances require it to stop the successive and new criminal behaviors.

KEYWORDS:

Undercover agent, computer undercover agent, grooming, sexting, child pornography.

ÍNDICE

ABREVIATURAS.....	Pág. 8
INTRODUCCIÓN.....	Pág. 9
CAPÍTULO 1: EL AGENTE ENCUBIERTO COMO DILIGENCIA DE INVESTIGACIÓN EN EL PROCESO PENAL	
1. Concepto.....	Pág. 11
2. Regulación.....	Pág. 11
3. Ámbito subjetivo.....	Pág. 13
4. Agente encubierto informático vs agente encubierto clásico.....	Pág. 17
4.1 Introducción.....	Pág. 17
4.2 Necesidad de respuestas diferenciadas.....	Pág. 18
4.3 Autorización judicial.....	Pág. 19
4.4 Ámbito objetivo.....	Pág. 20
5. Diferencias con el agente provocador y el confidente.....	Pág. 20
5.1 Diferencias con el agente provocador.....	Pág. 20
5.2 Diferencias con el confidente.....	Pág. 23
CAPÍTULO 2: ÁMBITO DE ACTUACIÓN DEL AGENTE ENCUBIERTO INFORMÁTICO Y MODUS OPERANDI	
1. Límites y garantías (DDFF).....	Pág. 26
1.1 Límites.....	Pág. 26
1.1.1 Principio de legalidad.....	Pág. 26
1.1.2 Principio de proporcionalidad.....	Pág. 27

1.1.3 Principio de subsidiariedad.....	Pág. 29
1.1.4 Principio de especialidad.....	Pág. 30
1.2 Garantías.....	Pág. 30
1.2.1 Garantía al derecho fundamental a la intimidad...	Pág. 30
1.2.2 Garantía al derecho fundamental al secreto de las comunicaciones.....	Pág. 32
1.2.3 Garantía al derecho fundamental a la defensa....	Pág. 33
2. Forma de proceder en la fase de investigación y actuaciones que puede llevar a cabo.....	Pág. 34
2.1 Crear un perfil en un foro y conversar en él autorizado bajo identidad ficticia.....	Pág. 35
2.2 Abrir cuentas corrientes y comerciar electrónicamente....	Pág. 36
2.3 Acceso a teléfonos asociados a las direcciones de IP.....	Pág. 37
2.4 Entrega de archivos que contengan material delictivo.....	Pág. 37
2.5 Interacción de la infiltración informática con el mundo físico.....	Pág. 37
3. Intervención del agente en la fase de juicio oral.....	Pág. 38

CAPÍTULO 3: ESPECIAL REFERENCIA AL AGENTE ENCUBIERTO INFORMÁTICO EN CASOS DE GROOMING Y PORNOGRAFÍA INFANTIL

1. Concepto de grooming, su relación con la pornografía infantil y el papel de las nuevas tecnologías en ellos.....	Pág. 41
2. Regulación de ambas figuras.....	Pág. 44
3. Modo de actuación por el agente encubierto.....	Pág. 46

CONCLUSIONES.....Pág. 51

BIBLIOGRAFÍA..... Pág. 54

ABREVIATURAS

CE: Constitución Española

CNI: Centro Nacional de Inteligencia

CNP: Cuerpo Nacional de Policía

CP: Código Penal

DDFF: Derechos Fundamentales

GC: Guardia Civil

LECrim: Ley de Enjuiciamiento Criminal

LO: Ley Orgánica

Pág.: página

SECED: Servicio Central de Documentación

STC: Sentencia del Tribunal Constitucional

STEDH: Sentencia del Tribunal Europeo de Derechos Humanos

STS/SSTS: Sentencia/s del Tribunal Supremo

SVA: Servicio de Vigilancia Aduanera

TC: Tribunal Constitucional

TEDH: Tribunal Europeo de Derechos Humanos

TFG: Trabajo de Fin de Grado

TS: Tribunal Supremo

TSJCyL: Tribunal Superior de Justicia de Castilla y León

UE: Unión Europea

INTRODUCCIÓN

La infiltración como método de indagación ha sido utilizado a lo largo de la historia, tanto por grupos particulares para conocer los entresijos de otros grupos rivales, como desde los poderes del Estado para introducirse en diferentes organizaciones criminales o grupos terroristas y tratar de acabar con ellos. Uno de los ejemplos más conocidos fue la infiltración de Mikel Lejarza, más conocido como “el Lobo”, el cual siendo agente del SECED¹ se infiltró en la cúpula de ETA político-militar, acabando con ella en 1975. No obstante, desde la promulgación de la LO 5/1999 de 13 de enero, (en adelante, LO 5/1999)² se reguló este ámbito con la inclusión del art. 282 bis de la Ley de Enjuiciamiento Criminal en el que se crea la figura del agente encubierto.

Con la incorporación del agente encubierto al ordenamiento jurídico español se dotó a la infiltración policial como diligencia de investigación de las garantías requeridas en un Estado de Derecho, ante una medida que, en ocasiones, lesiona los derechos fundamentales del investigado. Además, se reguló quién puede llevar a cabo este cometido bajo una identidad supuesta, los delitos perpetrados por grupos de criminalidad organizada que pueden investigarse o las actuaciones que puede realizar el agente una vez infiltrado.

Sin embargo, la realidad nunca permanece inmutable y, sobre todo, con la llegada del Siglo XXI, el progreso tecnológico sufrió un desarrollo vertiginoso. Ello supuso la aparición de Internet, un medio capaz de interconectar personas de todo el mundo. Pero, como ocurre en casi cualquier ámbito, no todo lo que rodea Internet iba a ser beneficioso. Pronto se vio que la otra cara de la moneda de esta herramienta dotaba de un amplio margen a los delincuentes para cometer con mayor facilidad algunos delitos, e, inclusive, llevar a cabo figuras delictivas nuevas. De tal manera que, el Derecho se vio obligado a adaptarse a esta nueva situación, aunque relativamente tarde y ciertamente insuficiente, como veremos. Para ello, entre las muchas modificaciones que se elaboraron, apareció

¹ Servicio Central de Documentación. Fue el servicio de inteligencia anterior al CNI durante la etapa final de la dictadura franquista.

² LO 5/1999 de 13 de enero, de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves, (BOE de 14 de enero de 1999).

con la LO 13/2015 de 5 de octubre³ (en adelante, LO 13/2015), el agente encubierto informático.

Mediante la realización de este Trabajo de Fin de Grado (TFG), trataremos de mostrar la importancia de la medida del agente encubierto informático en la actualidad y la necesidad de una continua adaptación a los avances incesantes que se producen en el mundo tecnológico. Ello, siempre desde una perspectiva jurídica, poniendo de manifiesto la necesidad de una actuación en respeto de los principios constitucionales, procesales y penales, así como la garantía de los derechos fundamentales que todo investigado debe poseer en cualquier investigación ante un presunto delito.

Para alcanzar este propósito, hemos dividido el TFG en tres capítulos. En el primero de ellos, mostraremos los antecedentes, previos a la aparición de la figura informática del agente encubierto, su regulación y presupuestos, las principales diferencias entre el agente encubierto físico e informático, donde nos meteremos de lleno en el estudio del agente en el ámbito informático y, por último, las diferencias con dos figuras próximas a la de agente encubierto que pueden confundirse con este, cuando son totalmente autónomas y diferentes.

En segundo lugar, observaremos los principios que, necesariamente, deberá respetar la acción del agente encubierto informático, así como los derechos fundamentales en juego de los investigados y las preceptivas autorizaciones adicionales en cada caso que deban provenir del juez. Nos centraremos, posteriormente en las actuaciones que, específicamente, se contemplan para el agente encubierto informático y veremos su importancia en las fases de instrucción y en el juicio oral.

Finalmente, con la intención de exponer la peligrosidad existente en delitos informáticos, principalmente en menores de edad, pondremos de manifiesto a modo ejemplificativo la posible actuación del agente encubierto informático en los delitos de grooming y relativos a la pornografía infantil, describiendo, con anterioridad, en que consisten ambos delitos y contemplando su regulación.

³ LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, (BOE de 6 de octubre de 2015).

CAPÍTULO 1: EL AGENTE ENCUBIERTO COMO DILIGENCIA DE INVESTIGACIÓN EN EL PROCESO PENAL

1. Concepto

La sentencia del Tribunal Supremo 1140/2010 de 29 de diciembre lo define como “el policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la Ley y bajo el control del Juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación o estos sean manifiestamente insuficientes, para su descubrimiento y permite recabar información sobre su estructura y modus operandi, así como obtener pruebas sobre la ejecución de hechos delictivos”⁴

Es decir, el agente encubierto es un funcionario perteneciente a la Policía Judicial que, siguiendo lo dictado por la ley y el Juez, procede a la infiltración en grupos de delincuencia organizada, siendo el caso paradigmático los de tráfico de drogas, para detectar la comisión de hechos delictivos que no han podido ser captados mediante la realización de otras diligencias de investigación.

Por tanto, el objetivo de estos agentes será la infiltración, consistente en la adopción de una identidad distinta a la suya propia, con la que puedan obtener un acercamiento, dentro de los grupos de criminalidad organizada, con los presuntos delincuentes que posibilite recabar la información suficiente para atribuirles la comisión de delitos y que, de esta forma, puedan ser juzgados por ellos.

2. Regulación

A lo largo de las últimas décadas, la regulación, primeramente, del agente encubierto y, posteriormente, del agente encubierto informático ha pasado de ser insuficiente y ciertamente criticada por la doctrina a comenzar a tratar los cambios sociológicos, pero sobre todo tecnológicos que, inexorablemente, van copando la sociedad y que, por tanto, han de ser recogidos en los ordenamientos jurídicos.

⁴ STS 1140/2010, Sala II, Sección 1ª, de 29 de diciembre de 2010, FJ 6º.

En España, el agente encubierto encargado de infiltraciones físicas aparece reglamentado en el art. 282 bis Ley de Enjuiciamiento Criminal (en adelante, LECrim) tras la reforma de esta Ley mediante la LO 5/1999. Esta supuso un gran avance, necesario porque era indispensable una regulación de esta figura, pero insuficiente y algo confusa, debido a que incluía una lista cerrada (*numerus clausus*) como entiende RIFÀ SOLER⁵ y desfasada de delitos propios para la investigación, por parte de un agente encubierto, en los que no se incluía la posibilidad de su utilización en multitud de delitos tecnológicos que con el paso de los años entraron en un gran auge.

No fue hasta la promulgación de la LO 13/2015, tras el fallido intento del proyecto del Código Procesal Penal de 2012, que se colmaron algunos vacíos legales relativos a los avances en las nuevas tecnologías, aunque, como expone BUENO DE MATA⁶ “a día de hoy, podemos considerar que el principio de legalidad sigue siendo una utopía”. Afirmación, que, por mi parte comparto, ya que, por mucho esfuerzo que se haya realizado, no se han incluido regulaciones ante elementos informáticos que, antes o después deberemos tratar. Todo ello, porque el Derecho no avanza con la misma rapidez que la tecnología, principalmente por voluntad del legislador y, sobre todo, por la dificultad que implica aprobar una ley en la actualidad.

De todas formas, es en esta ley donde se regula, entre otros elementos, por primera vez al agente encubierto informático mediante la adición de dos apartados en el art. 282 bis LECrim.

No debemos olvidar que, como diligencia de investigación que afecta a derechos fundamentales, debe respetar ciertos límites que marca la Constitución Española (en adelante, CE) y que veremos con posterioridad, por lo que no podemos hablar acerca de la regulación de este elemento pasando de preceptos tan importantes como son el art. 10 CE sobre la dignidad de las personas, el art. 18 CE en torno a la garantía de la intimidad

⁵ RIFÀ SOLER, J.M., “El agente encubierto o infiltrado en la nueva regulación de la LECrim.”, *Poder Judicial*, núm. 55, pág. 161.

⁶ BUENO DE MATA, F., “Fortalecimiento de Garantías procesales y medidas de investigación tecnológica”, *Ars Iuris Salmanticensis*, vol. 4, (2016), pp. 326 a 328, p. 326.

de las personas y el art. 24 CE relativo, entre otros derechos, al respeto del proceso con todas las garantías.

Por último, cabe destacar la normativa existente sobre el agente encubierto y agente encubierto informático en Derecho Internacional, que afecta al ordenamiento jurídico español y contempla la infiltración policial desde puntos de vista más específicos. Es el caso de la Convención de las Naciones Unidas contra la corrupción en su art. 50⁷ o la Convención de las Naciones Unidas de la Delincuencia Organizada Internacional en su art. 20⁸. De la misma manera, dentro del Derecho de la Unión Europea (en adelante, UE) es imprescindible referenciar la Directiva 2014/41/CE⁹ en su art. 29, que sustituye al Convenio Asistencial Judicial en materia penal entre los Estados Miembros de la UE¹⁰.

3. Ámbito subjetivo

Si atendemos a los casos de delincuencia organizada del art. 282 bis apartado 4 relativos para el agente encubierto físico o a delitos cometidos en canales cerrados de comunicación expuestos en el art. 282 bis apartado 6 para el agente encubierto informático, extraemos que cabe, si lo entiende conveniente la autoridad judicial o el fiscal encargado del caso, la autorización para la infiltración por parte de un agente de la Policía Judicial con el fin de obtener pruebas suficientes que permitan enfrentar la investigación de un supuesto delito.

Ahora bien, no es suficiente con decir que la Policía Judicial estará legitimada para llevar a cabo esta diligencia, debido a que es indispensable recoger qué funcionarios de los cuerpos concretos que pertenecen a este grupo pueden llevar a cabo estas funciones. Es, por ello, que, en principio, deberíamos acudir al art. 283 LECrim en el que se desglosa aquellos grupos constituyentes de la Policía Judicial.

⁷ Convención de las Naciones Unidas contra la corrupción, art. 50, Mérida, 2003.

⁸ Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos, art. 20, Palermo, 2000.

⁹ Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal (DOCE 1 de mayo de 2014)

¹⁰ Convenio de asistencia judicial en materia penal entre Estados miembros de la Unión Europea (establecido mediante Acto del Consejo de 29 de mayo del 2000, DOCE C 197 de 12.07.2000).

En cambio, tras una lectura textual del artículo, es sencillo darse cuenta de la necesidad de reforma que ha de pesar sobre él, como declara CARRIZO GONZÁLEZ-CASTELL¹¹. En él, se incluyen como formantes de la Policía Judicial, cuando realmente no lo son, a Alcaldes, Tenientes de Alcaldes, Serenos, Celadores o Guardas de montes entre muchos otros. Estos, como ahora veremos, en ningún caso podrán desempeñar el papel de agentes encubiertos. Ante esto, podemos realizar la misma reflexión aportada sobre la LO 13/2015, en torno a la incapacidad del poder legislativo de adaptar las leyes a la realidad actual.

Tendremos que acudir al Real Decreto 769/1987 de 19 de junio¹², en su art. 1 y 7, donde se alude que constituirán esta Policía, las Fuerzas y Cuerpos de Seguridad del Estado.

Partiendo de este punto, solo podrán ejercer como agentes encubiertos los pertenecientes a la Policía Judicial que de forma totalmente voluntaria ocupen un puesto¹³:

1. Como agentes del Cuerpo Nacional de Policía (CNP).
2. Como miembros de la Guardia Civil (GC).
3. Como agentes de las Policías Autonómicas, en el caso de que estas tengan competencias para ser policía judicial en sus correspondientes Estatutos de Autonomía, siendo así la Ertzaintza, el cuerpo de Mossos d'Esquadra y la Policía Foral de Navarra. Eso sí, todos estos grupos no podrán actuar como agentes encubiertos en investigaciones de carácter internacional, ya que a efectos de la UE no son considerados policía "Schengen"¹⁴ por no tener competencias en todo el Estado.

¹¹ CARRIZO GONZÁLEZ-CASTELL, A., "La infiltración policial en España como medio de investigación en la lucha contra la corrupción". *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 3, n. 2, pp. 511-536, p. 518.

¹² Real Decreto 769/1987, de 19 de junio, sobre regulación de la Policía Judicial, (BOE de 24 de junio de 1987)

¹³ POZO PÉREZ, M. DEL, "El agente encubierto como medio de investigación de la delincuencia organizada en la ley de Enjuiciamiento Criminal Española", *Criterio jurídico*, vol.6, Santiago de Cali, 2006, p. 287.

¹⁴ Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 19 de

Así, quedarán descartados para realizar estas funciones entre otros:

1. Agentes de la Policía Local de los diferentes municipios.
2. Agentes del Centro Nacional de Inteligencia (CNI) a efectos de los márgenes dotados por la LECrim, porque sí cuentan con funciones de infiltración, pero con fines y parámetros de actuación distintos.
3. Agentes del Servicio de Vigilancia Aduanera (SVA)

Una vez estudiado los diferentes miembros de la Policía Judicial que podrán ejercer como agente encubierto, no debemos dejar de lado el perfil y formación con el que debe contar este. No cualquier agente del CNP, GC o policías autonómicas estará capacitado para un papel tan delicado. Deberá reunir una serie de características¹⁵ tales como una buena capacidad de decisión, solución de problemas y adaptación al medio, eficacia y competencia, inteligencia (incluida la emocional), ser empático, seguro de sí mismo, con aptitud para asumir riesgos sin la pérdida del control, preferentemente sin mujer e hijos y con una edad comprendida entre los 25 y 45 años.

Considero que es importante proyectar una situación real en la que a un agente le haya sido encomendado la infiltración en una organización criminal. Sin, al menos reunir estas características, el porcentaje de que este no sea descubierto por alguna persona que forma parte del entramado de la organización es muy bajo.

Además de todo lo dicho, tendrá que contar con una formación jurídica, técnica y tecnológica, psicológica, formación específica en aspectos de seguridad, prácticas de campo y, si fuese necesario, en ciertos idiomas relacionados al caso.

Con respecto al agente encubierto informático, es necesario mostrar que las aptitudes indispensables para ocupar una figura o la otra variarán en cierta medida. Lo que no implica que no sean, únicamente, los integrantes de la Policía Judicial quienes vayan a estar legitimados para ocupar este puesto como agente encubierto informático.

junio de 1990, al cual se adhirió el Reino de España mediante el Acuerdo de Adhesión de España el 25 de junio de 1991.

¹⁵ POZO PÉREZ, M. DEL, “El agente encubierto... op., cit., p. 289 y 290.

Ya hemos tenido en consideración que el agente encubierto ha de tener unas características físicas acordes al requerimiento de la investigación. No obstante, estos requisitos pasan a tener un papel secundario en favor, como declara RIZO GÓMEZ, de altos conocimientos de informática y, por consiguiente, de internet y una importante fortaleza psíquica, contando con ayuda psicológica para el caso de que sea necesario. Hemos de destacar que el grado de formación y de preparación del agente encubierto informático resulta crucial para la tarea que tiene cometida resulte exitosa¹⁶.

Por ello, como indica BUENO DE MATA¹⁷, el perfil más adecuado en la Policía Judicial para llevar a cabo la función de agente encubierto informático lo presentan los integrantes de la Brigada de Investigación Tecnológica, tanto del Cuerpo Nacional de Policía como de la Guardia Civil.

Eso sí, además de la obvia necesidad de un dominio importante sobre la informática, el agente encubierto informático tendrá que contar con aptitudes psicológicas diferenciales como capacidad de persuasión, disposición sin titubear a la toma de decisiones y facultades emocionales como la empatía o la mesura, sabiendo adaptarse a lo que requiere cada situación¹⁸.

A mi parecer, sería complejo que un agente reuniese las características necesarias de la figura clásica y tecnológica, porque como hemos comprobado, la doctrina nos revela la importancia en el cumplimiento de esas características que, debido a su especificidad, conlleva a que muy pocos tengan estas particularidades, solo, en referencia a una tipología de agente.

¹⁶ RIZO GÓMEZ, M. B. “La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica” en *Justicia Penal y nuevas formas de delincuencia*, Tirant Lo Blanch, Valencia, 2017, p. 108.

¹⁷ BUENO DE MATA, F., “El agente encubierto en Internet: Mentiras virtuales para alcanzar la justicia”, *Los retos del Poder Judicial ante la sociedad globalizada*, Universidade da Coruña, A Coruña, 2011, p. 301.

¹⁸ BUENO DE MATA, F., *Las diligencias de investigación penal en la cuarta revolución industrial*, Thomson Reuters Aranzadi, Cizur Menor, 2019, p. 116.

Ahora bien, el hecho de que una persona pueda reunir la mayoría o, incluso todas las características que la doctrina ha entendido como necesarias para ambas figuras, no va a suponer, de primeras, que el policía se encuentre desde ese punto capacitado para infiltrarse, sin antes recibir una formación específica del trabajo que va a llevar a cabo y concretamente del caso que se le asigne¹⁹.

Por ello, la conclusión a la que debemos llegar se basa en entender que tanto la condición de Policía Judicial, como las características específicas para uno u otro tipo de agente, ayudan a que existan más probabilidades de obtener el fin pretendido con la aplicación de esta medida para un supuesto concreto, pero, en ningún momento está garantizado alcanzar el resultado querido, ya que nos estamos enfrentando a grupos de criminalidad organizada e individuos veteranos en la comisión delictiva, los cuales cada vez tienen menos confianza en aquellos que se interesan por sus actividades, porque, sin duda conocen el ordenamiento y la posibilidad de aplicar estas diligencias.

4. Agente encubierto informático vs. Agente encubierto clásico

4.1 Introducción

Como expone FERNÁNDEZ TERUELO²⁰, “el derecho penal y el procesal (penal) vigentes, así como los principios garantistas inherentes a ambos, han sido contruidos, en esencia, sobre la base de un modelo de criminalidad física, marginal e individual. Frente a ello, con la aparición de internet, los distintos organismos encargados de su represión se han debido enfrentar a un cauce de ejecución delictiva que cuestiona plenamente muchos de los axiomas vigentes”

En un intento de paliar ese cauce de ejecución delictiva, apareció la ya referenciada LO 13/2015, introduciendo, entre otros instrumentos, la figura del agente encubierto informático en las disposiciones de la LECrim²¹. Aunque ambas figuras son similares en

¹⁹ POZO PÉREZ, M. DEL, “El agente encubierto como medio de investigación...”, op., cit., p. 290.

²⁰ FERNÁNDEZ TERUELO, J. G., “Cibercrimen. Los delitos cometidos a través de internet” *Constitutio Criminalis Carolina*, Oviedo, 2007, p. 13.

²¹ Art. 282 bis apartados sexto y séptimo.

ciertos aspectos, podemos destacar a partir de la lectura del precepto y con una visión global de la función de ambas figuras, puntos de vista diferenciados.

4.2 Necesidad de respuestas diferenciadas

Como ya hemos manifestado, los motivos por los que la LO 13/2015 fue elaborada se fundan en razones de urgencia y necesidad, tratando de eliminar las lagunas que provenían de la LO 5/1999²². Ello es así, por las posibilidades que dota internet a sus usuarios.

En primer lugar, un delincuente que actúe fuera del ciberespacio, aunque trate de ocultarse y mantenerse ajeno a todo lo que le rodea para evitar ser observado por el resto de personas, más o menos cercanas a él, no tiene la facultad de anonimato que puede ofrecer internet, donde la apariencia física de quienes lo utilizan queda relegada en pos de meros “nicks” en foros o el único rastro que puede dejar una dirección IP.

No obstante, el anonimato de internet puede ser aun mayor que el que puede alcanzar cualquier usuario a pie de calle si accede al internet profundo, más conocido como “Deep Web” o la estructura dentro de esta, utilizada para delinquir llamada internet oscuro o “Dark Web”. MARTÍN IBÁÑEZ²³ indica que la Deep web es la parte más grande de internet, a la que no se puede acceder desde los buscadores web convencionales (google, yahoo, etc), siendo necesario herramientas específicas para poder acceder. Ambas constituyen una importante fuente de ciberinteligencia, sobre todo en torno a amenazas, vulnerabilidades y riesgos.

De tal manera que, aquellos que se adentran en la “Dark Web” y tienen los conocimientos necesarios para no ser detectados, pueden llegar a pasar totalmente inadvertidos, ya que también queda oculta su dirección IP. Debido a esto, muchas redes organizadas y delincuentes solitarios utilizan esta zona de internet para delinquir sin ser descubiertos. Por ello, la figura del agente encubierto informático se hace fundamental.

²² BUENO DE MATA, F., “Fortalecimiento de garantías procesales...”, op., cit., p.326 y 327

²³ MARTÍN IBÁÑEZ, E., “Dark web y Deep web como fuentes de ciberinteligencia utilizando minería de datos”, *Cuadernos de la Guardia Civil: Revista de seguridad pública*, nº 54, 2017, p. 74.

En segundo lugar, y pese a que como hemos dicho la mayoría de hechos delictivos se producen en el internet oscuro, es, lamentablemente, muy común, la comisión de delitos tales como el *grooming* que se producen en las redes sociales más conocidas y utilizadas de internet. Ello se debe, en parte, a la carente conciencia y cuidado que mantienen los internautas en comparación con sus actuaciones en el mundo real, lo que denota la exigencia de la figura del agente encubierto informático en contraposición a la figura clásica, reservada como veremos para otro tipo de situaciones, al existir comúnmente esa cautela.

En tercer lugar, la figura del agente informático, al contrario que la clásica tiene un carácter transnacional más marcado. Ciertamente es que en los últimos años la delincuencia organizada, principalmente el narcotráfico, ha ampliado sus fronteras con instrumentos que permiten la delincuencia internacional. No obstante, internet concede la posibilidad, de manera mucho más sencilla, de hacerlo con un simple clic. De ahí, la obligación de agentes informáticos con los conocimientos necesarios y con la suficiente capacidad de coordinación con aquellos que se dedican al mismo desempeño.

4.3 Autorización judicial

Si atendemos a la literalidad del art. 282 bis apartado primero LECrim, observamos que un agente encubierto físico podrá ser autorizado a actuar como tal por el Juez de Instrucción competente o por el Ministerio Fiscal, si este da cuenta inmediata al Juez. Sin embargo, el art. 282 bis apartado sexto LECrim indica que solo el Juez de Instrucción podrá autorizar al agente encubierto informático para ejercer ese cometido.

Esta diferencia tiene un trasfondo esencial, porque se fundamenta en el hecho de que solo el Juez está capacitado para instaurar medidas que conlleven restricción de LO²⁴. Algo que se produce por la posibilidad con la que cuenta el agente encubierto informático para la grabación de comunicaciones y obtención de imágenes, para lo cual, resulta preceptivo una ampliación de la medida anterior con la que contaba el agente

²⁴ BERNARDO SAN JOSÉ, A. “La restricción de los derechos fundamentales en las diligencias de investigación en el proceso penal y las exigencias derivadas del principio de proporcionalidad”, *Revista Ius*, Vol. 3, nº 24, 2009.

informático²⁵. Es decir, el agente encubierto informático resulta un instrumento que, en sí mismo, supone una restricción de derechos fundamentales al afectar al derecho fundamental del secreto de las comunicaciones²⁶, mientras que, el agente encubierto clásico cuenta con una serie de movimientos más amplio que no da lugar, en muchos casos, a la restricción de estos derechos, pese a que pueda ser autorizado por el Juez de Instrucción igualmente para ello²⁷.

4.4 Ámbito objetivo de actuación

El agente encubierto informático y el agente encubierto clásico comparten la posibilidad de actuación en torno a los delitos relativos a la criminalidad organizada que contempla el art. 282 bis apartado 4 LECrim. Pese a ello y, a diferencia de lo que ocurre con la modalidad “ordinaria” de agente encubierto, el informático puede desempeñar su función con el objetivo de investigar hechos delictivos previstos en el art. 588 ter a LECrim²⁸.

Este artículo a su vez contiene una referencia por la cual el agente encubierto informático resulta competente para indagar en los delitos que aparecen en el art. 579.1 LECrim. Este incluye la investigación de “Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión, delitos cometidos en el seno de un grupo u organización criminal o delitos de terrorismo”. De aquí extraemos que se produce una flexibilización en el ámbito objetivo con respecto a la otra modalidad al permitir el uso de esta diligencia más allá de delitos de delincuencia organizada.

5. Diferencias con el agente provocador y el confidente

5.1 Diferencias con el agente provocador

Es muy común que aquellos que comienzan en el estudio de la infiltración policial como diligencia de investigación confundan, en un primer momento, la figura del agente

²⁵ Art. 282 bis apartado séptimo LECrim.

²⁶ Art. 18.3 Constitución Española.

²⁷ STS 750/2019, Sala II, Sección 1ª, de 13 de marzo de 2019, F. J. 2º.

²⁸ Art. 282 bis apartado sexto LECrim.

encubierto con la del agente provocador. Sin embargo, hemos de reseñar que son dos elementos claramente diferenciados, cuyas funciones y, por tanto, finalidades, disienten entre sí.

Para entender qué es un delito provocado por un agente, acudimos a la jurisprudencia más reciente sobre ello por parte del TS. “ El delito provocado es aquél que llega a realizarse en virtud de la inducción engañosa de un agente que, deseando conocer la propensión al delito de una persona sospechosa y con la finalidad de constituir pruebas indubitables de un hecho criminal, convence al presunto delincuente para que lleve a cabo la conducta que de su torcida inclinación se espera simulando primero allanar y desembarazar el *iter criminis* y obstruyéndolo finalmente, en el momento decisivo, con lo cual se consigue que por el provocador no sólo la casi segura detención del inducido sino la obtención de pruebas que se suponen directas e inequívocas”²⁹

Es decir, para que se produzca un delito provocado por un agente, la comisión del hecho delictivo ha de provenir de la iniciativa del agente provocador, cuyo objetivo es inducir a la persona que se esté provocando a que, efectivamente, lleve a cabo un delito. El fin de esta acción del agente no es otra que detener al provocado tras la realización de la acción delictiva, lo que implica que la única predisposición del agente para provocar el delito es la subsiguiente detención del presunto delincuente.

No obstante, más allá de la intención del agente, es indispensable, para que tenga lugar esta figura, la existencia de la voluntad y posterior puesta en disposición de las medidas preventivas necesarias por parte de este, para que el resultado propio del delito cometido no llegue a buen puerto.

Por ello, la diferencia más importante, quizá, entre el agente provocador y el agente encubierto reside en que el primero, desde su ámbito personal, hace porque se produzca el hecho delictivo. Este no surge de la esfera de los delincuentes, debido a que, si la actuación de los agentes solo implica la investigación y revelación de esta conducta mediante la infiltración, sin la intención de provocar ellos el delito, estaremos ante el encubierto³⁰.

²⁹ STS 2331/2021, Sala II, Sección 1ª, de 10 de junio de 2021, F.J. 4º.

³⁰ STS 679/1998, Sala II, Sección 1ª, de 28 de julio de 1998, F. J. 22º.

Realmente, para que aparezca la persona del agente provocador no ha de existir con carácter previo un delito y, sin embargo, la función del agente infiltrado no puede tener lugar sin que el hecho delictivo ya exista, presuntamente. Y, además, este provenga del deseo de su comisión de los autores, diferentes al agente³¹.

Un punto de vista significativo que permite entender fácilmente la distinción entre los dos agentes tiene como base el momento de actuación de un agente y otro. Un agente encubierto lleva a cabo la conducta necesaria con respecto a la investigación en curso, inmediatamente después de que empiecen a moverse los investigados. Por otro lado, el agente provocador es el primero en actuar, sembrando el propósito de delinquir en los sujetos provocados.

A diferencia del agente encubierto, para cuya posición es necesario formar parte de la Policía Judicial, para el agente provocador no es imprescindible, por lo que cualquier agente de policía, podrá realizar esta función³². En adición a esto y, siguiendo con los requerimientos propios del infiltrado, un agente provocador no deberá contar con una identidad falsa o una autorización judicial para el cumplimiento de su cometido, simplemente no exhibirá su condición policial.³³

El agente provocador no se infiltra en una organización criminal, sino que simplemente busca un cierto trato o comunicación con alguno de sus integrantes, lo que supone que la relación que tiene este agente con los formantes de la organización es mínima. Ello implica que la posibilidad de que se den vulneraciones de derechos fundamentales es más baja que en el caso del agente infiltrado.

Como contempla MOLINA PÉREZ, T.³⁴ uno de los supuestos que más controversia generan en relación con estas figuras se produce cuando para el agotamiento o consumación de un delito se ofrece un policía fingiendo ser delincuente. En esta situación

³¹ STS 690/2010, Sala II, Sección 1ª, de 1 de julio de 2010, F. J. 12º.

³² STS 1114/2002, Sala II, Sección 1ª, de 12 de junio de 2002, F. J. 1º.

³³ PERALS CALLEJA, J., “Técnicas de investigación del crimen organizado: el agente encubierto, confidente, regulación en España y validez de la prueba obtenida en el extranjero, problemas prácticos de la heterogénea regulación de la materia”, Cuadernos Digitales de Formación, 2010, p. 18.

³⁴ MOLINA PÉREZ, T., “Técnicas especiales de investigación del delito. El agente provocador, el agente infiltrado y figuras afines”, “Anuario Jurídico y Escurialense, XLII, 2009, p. 158.

no estamos ante una provocación de delito, para la cual es necesario que no sea el autor el que decidiese cometerlo, ni tampoco ante un supuesto de infiltración. Solamente queda enmarcado dentro de las funciones contempladas para la Policía judicial en el art. 283 LECrim.

En definitiva, la dialéctica entre la figura del agente provocador y el agente encubierto ha sido tenida en cuenta por los tribunales con más peso, no solo nacional, sino también internacional. Destaca así, la doctrina del TEDH, el cual de manera recurrente en todos los casos ha determinado que no cabe incluir en un proceso penal la prueba que se haya recabado mediante la provocación delictiva realizada por un agente, al contrario de lo que ocurre con el agente encubierto³⁵.

Para tratar de evitar que se produzca una confusión y un agente nombrado como encubierto acabe provocando un delito, el TEDH ha incidido en la necesidad de que los Estados cuenten con una legislación que no dé lugar a dudas en la que, sobre todo, se exponga claramente que el control sobre la acción de infiltración provenga por parte del juez y no así de superiores policiales, porque su desconocimiento técnico en este ámbito da lugar en muchos casos a la provocación delictiva³⁶.

5.2 Diferencias con el confidente

El confidente es aquel individuo que proporciona información a la policía a cambio de dinero o algún trato de favor por parte de los agentes³⁷. Con carácter general, el confidente tiene relación con ambientes criminales o delictivos, lo que le permite llevar a cabo esta función de la manera más deseable posible³⁸.

A raíz de esta definición, extraemos la primera diferencia y puede que la más importante entre este y al agente encubierto. La figura del confidente puede ser ocupada por cualquier persona, no siendo necesario la condición policial que conocemos que ha

³⁵ STEDH de 5 de febrero de 2008. Asunto Ramanauskas contra Lituania, Gran Sala, nº18757/2006.

³⁶ Un ejemplo de ello lo contemplamos en un caso solventado por la SAP de Navarra, Sección 2ª, nº256/2016 de 14 de diciembre de 2016.

³⁷ GIMENO SENDRA, V., (MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V.), *Derecho Procesal Penal*, Colex, Madrid, 1999, p. 409.

³⁸ Un ejemplo paradigmático de confidente es el del interno en prisión que comparte información con los agentes de policía a cambio de algún beneficio penitenciario.

de tener el agente encubierto. Este elemento ha de tenerse muy en cuenta, puesto que el confidente para la puesta a disposición de la información a la policía, tal vez, deba infiltrarse allá donde se estén produciendo hechos delictivos, lo que puede llevarnos a confusión. Eso sí, podrá actuar, igualmente, aportando cualquier dato sobre un hecho pasado del que tuviese conocimiento o en el que estaba inmerso.

El ámbito de actuación del confidente, a diferencia del agente encubierto, no queda relegado a la criminalidad organizada, sino que también puede ser empleado en otras modalidades comunes de delito, en los que, aunque cabe su comisión por un grupo criminal, es común su puesta a punto por individuos que actúan en solitario o de forma conjunta, pero no bajo la organización de tales grupos criminales.

En el supuesto de que un confidente se infiltre para llevar a cabo su función, su identidad podrá permanecer oculta con respecto a aquellos relacionados con el delito al momento de la infiltración, no así en el posible proceso posterior en el que pueda participar como testigo referencial, donde su anonimato no será comparable al de un agente encubierto en este ámbito. El confidente deberá mostrar su identidad ante el juez como la persona que ha dotado de los datos necesarios para la declaración directa del policía en el juicio, con la única opción de poder acogerse a la protección de testigos³⁹.

El valor probatorio que evidencia lo averiguado o traído por el confidente es inferior al testimonio de un agente encubierto, ya que el de este último pesa como una pieza de convicción más, junto con todas aquellas de más que puedan resultar determinantes para una eventual sentencia condenatoria, mientras que, aquello obtenido por el confidente podrá ser tratado como indicio que necesitará ser comprobado y aportado mediante declaración en juicio por el agente de policía que recibe la información del confidente.

Tal es así, que, el ámbito de actuación del confidente puede que se desarrolle con carácter externo y previo al proceso, existiendo la posibilidad de que sea de utilidad para la apertura de la fase de diligencias. No obstante, hemos de traer a colación algo ya comentado y es que la infiltración del agente encubierto se hace una vez iniciado el

³⁹ ZAFRA ESPINOSA DE LOS MONTEROS, M.R., *El policía infiltrado: los presupuestos jurídicos en el proceso penal español*, Tirant Lo Blanch, 2010, p. 134.

proceso penal, constituyéndose de por sí como una diligencia de investigación de primera mano⁴⁰.

Ahora bien, hemos de tener en cuenta que cabe la posibilidad de un trabajo conjunto entre el agente encubierto y el confidente, ya que, en muchas ocasiones, este último se encargará de transmitir la existencia de un grupo de criminalidad organizada o foro en el que sea necesaria la aparición de un agente encubierto, donde puede llegarse al caso en el que el confidente “apadrine” al agente para su entrada en el grupo, de tal forma que el resto de integrantes no desconfíen de él.

Por tanto y, aunque en un principio podría haber parecido que la figura del agente provocador guarda una mayor relación con el agente encubierto, es realmente el confidente el que, verdaderamente, de forma legal puede ayudar a introducir en el proceso, pese a que no sea directamente por sí mismo, piezas de convicción a través del agente encubierto.

Realmente, eso sí, la confusión es más entendible entre el agente encubierto y el provocador, sobre todo por su condición, en ambos casos, de policía, debido a que el confidente no es más que una persona cercana al delito que con una motivación u otra decide proporcionar información a las Fuerzas y Cuerpos de Seguridad del Estado.

⁴⁰ ZAFRA ESPINOSA DE LOS MONTEROS, M.R., *El policía infiltrado...*, op., cit., p.136.

CAPÍTULO 2: ÁMBITO DE ACTUACIÓN DEL AGENTE ENCUBIERTO INFORMÁTICO Y MODUS OPERANDI

1. Límites y garantías (DDFF)

1.1 Límites

1.1.1. Principio de legalidad

El sometimiento a la ley constituye un límite lógico y trasladable a cualquier actuación de las personas físicas y jurídicas e, igualmente, de los poderes públicos, ya que ello supone la base de un Estado de Derecho.⁴¹

Sabemos que el agente encubierto informático es una figura restrictiva de derechos fundamentales (en adelante, DDFF) en sí misma y, como tal, para llegar a obtener esa condición, es necesario que la ley prevea la posibilidad de que, con esta medida, se pueda dar paso a la limitación de estos derechos. Es decir, sin la inclusión en el ordenamiento jurídico de la aptitud del agente encubierto informático como medio limitativo de DDFF no existiría esta diligencia⁴².

El cumplimiento de este principio se materializa con la inclusión de su regulación en la ya reseñada LO 13/2015⁴³, como figura restrictiva de DDFF y, por supuesto, el art. 282 bis apartado sexto y séptimo de la LECrim. Ahora bien, la jurisprudencia toma una posición muy importante, ya que profundiza en cómo ha de ser la actuación del agente en cumplimiento de este principio. Según estima el TS en su sentencia 104/2019, la actuación procesal y sustantiva del agente encubierto para no desviarse de lo requerido por este principio, , ha de atender a “las razones de la solicitud policial para su nombramiento, la resolución que lo acuerda y condiciones establecidas, la constancia en autos de las actas levantadas, la inexistencia de delito provocado, la prestación de su declaración en juicio como testigo y, por tanto, sujeto a los principios imperantes del

⁴¹ Art. 25.1 CE.

⁴² GOMÉZ DE LIAÑO FONSECA-HERRERO, M., "Infiltración policial y proceso penal", Investigación y prueba en el proceso penal, N. González-Cuéllar Serrano y Á. Sanz Hermida (coords.), Madrid, 2006, p. 208.

juicio oral, singularmente, contradicción e inmediación, la entrega en el plenario de las actas levantadas por el agente en cuestión y la inexistencia de nulidad de las grabaciones llevadas a cabo por el agente encubierto”⁴⁴.

Este principio es, en definitiva, un elemento básico para dotar a los poderes públicos (y más concretamente a la justicia) de legitimidad democrática a la hora de actuar con una posible restricción de DDFF⁴⁵.

1.1.2 Principio de proporcionalidad

Si el principio de legalidad posibilitaba la existencia del agente encubierto informático, el de proporcionalidad tiene como función modular su actuación. De tal forma, que se relega su uso a situaciones muy concretas en las que aparezca una “utilidad” y “necesidad” que justifiquen su función. La STC 50/1995 entre muchas otras lo define como “una relación ponderada de los medios empleados con el fin perseguido, para evitar el sacrificio innecesario o excesivo de los derechos fundamentales, cuyo contenido esencial es intangible”.⁴⁶

Para que consideremos que existe la “utilidad” suficiente para aplicar esta figura ZAFRA ESPINOSA DE LOS MONTEROS entiende que “se alcanza cuando sea previsible la consecución del fin (adecuación cualitativa); cuando su intensidad en relación con el fin perseguido sea tolerada por el Estado (adecuación cuantitativa) y que esté individualizada”⁴⁷. Por tanto, con la mera posibilidad de obtener el desenlace deseado será suficiente para que hablemos de utilidad, no siendo obligatorio que la aplicación de esta diligencia termine llevándonos al resultado esperado en un primer momento.

⁴⁴ STS 104/2019, Sala II, Sección 1ª de 27 de febrero de 2019, F.J. 2º.

⁴⁵ GONZÁLEZ-CUELLAR SERRANO, N., *Proporcionalidad y derechos fundamentales el proceso penal*, Colex, Madrid, 1990, p. 69.

⁴⁶ STC 50/1995, Sala Primera, de 23 de febrero de 1995, F.J. 7º.

⁴⁷ ZAFRA ESPINOSA DE LOS MONTEROS, R., *El policía infiltrado*, op., cit., p. 380.

Por otro lado, la “necesidad” supone contemplar las medidas factibles a imponer para resolver el caso, debiendo escoger, entre la utilidad que todas aportan al caso, la que menos dé lugar a restringir los DDFF⁴⁸.

Estos dos elementos que han de concurrir en una misma diligencia se cumplen en el supuesto paradigmático del agente encubierto informático, como es la infiltración en grupos de pornografía infantil, debido a que es una situación oculta a cualquier otra forma de investigación menos lesiva de DDFF. Además, de ser la única útil, en la mayoría de los casos, para poder obtener pruebas ante un supuesto delito relacionado con esta pornografía.

La ampliación del ámbito objetivo de actuación del agente encubierto informático más allá de delitos cometidos por organizaciones y grupos criminales ha supuesto ventajas, pero múltiples inconvenientes. La STS 140/2019⁴⁹ nos permite comprobar aquello que la propia ley nos muestra por remisión del art. 282 bis apartado sexto LECrim, al art. 588 ter a LECrim y este a su vez al art. 579 LECrim, cuando expone que la figura de este agente se enfoca, además de a los delitos contemplados en el art. 282 bis apartado cuarto a “delitos de terrorismo, delitos cometidos en el seno de una organización criminal o delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; o cualquier otro delito cometido a través de medios informáticos”. Esta ampliación con respecto a la figura clásica permite la aplicación de esta medida para supuestos delictivos de mucha menor entidad.

Es muy común últimamente, la comisión del delito de estafa a través de Internet. Este tipo delictivo en la actualidad tiene una pena privativa de libertad de seis meses a tres años, lo que permitiría, en un principio, el empleo del agente encubierto informático como diligencia de investigación. No obstante, hemos de tener cuidado. Que exista una apertura de modalidades delictivas no implica que, en respeto a este principio de proporcionalidad, podamos hacer uso del agente en cualquiera de ellas. Siguiendo este ejemplo de la estafa, sería conveniente, antes siquiera de pensar en la infiltración policial a través de medios

⁴⁸ MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, McGraw-Hill, Madrid, 1996, p.128.

⁴⁹ STS 140/2019, Sala II, Sección 1ª, de 13 de marzo de 2019, F. J. 4º.

informáticos, hacerlo en el uso de otras herramientas de investigación que resulten mucho menos lesivas a los DDFF.

A mi parecer, el límite establecido por la ley no debe ser más que una referencia para que los jueces tengan un punto de partida desde donde el que poder observar, caso por caso, cuándo es necesario y útil el uso de esta medida. No podemos abrir su utilización a cualquier delito cometido a través de medios informáticos con un límite máximo de, al menos, tres años, porque de esa manera el empleo que estaríamos haciendo de la figura es absolutamente desproporcionado.

De hecho, mi posición está más cercana a lo que propone RIZO GÓMEZ, cuando argumenta que la gravedad del delito no debería atender a la pena, sino a la propia valoración del juez en el caso concreto. Tal es así que llega a proponer que disminuya ese límite máximo de tres años para que dependa en mayor medida de la decisión que tome el juez⁵⁰. Con esto último, sin embargo, no concuerdo. Creo que bajar el límite puede suponer un mayor número de confusiones y un aumento de probabilidad de que, efectivamente, se acabe aplicando la medida en un supuesto totalmente innecesario que lleve a una violación de DDFF.

1.1.3 Principio de subsidiariedad

Muy unido a este principio de proporcionalidad y sobre todo al requisito de necesidad, se sitúa el principio de subsidiariedad.

Este supone que la utilización de esta medida será dar solo de forma excepcional, cuando no exista otro medio procesal de investigación que permita perseguir el hecho delictivo. Así, deberán agotarse todas las vías posibles antes de acudir al agente encubierto informático, cuya disposición solo podrá ejercerse como “última ratio”. Por lo que deberá haber una sospecha sólida de que tendrá lugar un delito que solo podrá perseguirse probabilísticamente con la participación de este agente.⁵¹

⁵⁰ RIZO GÓMEZ, M. B., “La infiltración policial...op., cit., p. 114.

⁵¹ PAZ RUBIO, J. M^a; MENDOZA MUÑOZ, J.; MORICHE, R. R; OLLÉ SESÉ, M., *La prueba en el proceso penal. Su práctica ante los Tribunales*, Madrid, 1999.

Tal excepcionalidad radica en preservar las libertades de aquellos que se encuentren investigados, con la intención de que el Estado mantenga su calificativo “de Derecho”. De tal modo, que su utilización provenga solamente en pos de la seguridad colectiva, cuando el interés general se vea en peligro⁵²

1.1.4 Principio de especialidad

La propia exposición de motivos de la LO 13/2015 haciendo referencia a los principios proclamados por el TC⁵³, alude específicamente a este principio, obligando para la exigencia de su cumplimiento que “la actuación de que se trate tenga por objeto el esclarecimiento de un hecho punible concreto, prohibiéndose pues las medidas de investigación tecnológica de naturaleza prospectiva, de acuerdo con el concepto que informa la doctrina emanada del máximo intérprete de la Constitución, por todas la sentencia 253/2006, de 11 de septiembre”⁵⁴.

Con ello tratará de evitarse que los agentes encubiertos informáticos se infiltren de manera constante en diferentes grupos sin una sospecha cierta de la posible comisión de un delito⁵⁵, ya que ello corresponderá a las Brigadas Tecnológicas de la Policía Judicial, cuya función, entre otras, se fundamenta en lo que podríamos llamar desde mi punto de vista (en un plano informal) como “el patrullaje cibernético”.

Todo ello tiene la base en que, como ya conocemos, para que un agente pueda infiltrarse, necesitará para este supuesto la preceptiva autorización judicial ante la sospecha de un delito que ha de investigarse, no pudiendo, evidentemente, autorizarse genéricamente las infiltraciones sin causa y motivación.

1.2. Garantías

1.2.1 Garantía al derecho fundamental a la intimidad

⁵² SUITA PÉREZ, N., “La diligencia de investigación mediante la entrega vigilada”, *La actuación de la policía judicial en el proceso penal*, Madrid, 2006, p. 278.

⁵³ STC 253/2006, Sala Primera de 11 de septiembre de 2006, F. J. 2º.

⁵⁴ Exposición de motivos de la LO 13/2015.

⁵⁵ MOLINA MANSILLA, M. C., *Mecanismos de investigación policial: entrega vigilada y agente encubierto*, Barcelona, 2009, p. 32.

El derecho a la intimidad es un derecho fundamental que aparece contemplado en el art. 18 apartado primero de la CE y supone la capacidad de una persona para excluir del conocimiento y divulgación de su vida privada⁵⁶.

La aptitud para restringir el derecho a la intimidad por parte del agente encubierto informático varía en función del momento de la infiltración en el que nos encontremos⁵⁷. El primer momento en una infiltración clásica supondría el primer contacto entre el agente encubierto y los presuntos delincuentes, donde el agente, fingiendo querer mantener cualquier “operación comercial”, oculta su condición de policía.⁵⁸

Esta circunstancia puede ser trasladable a la figura del agente encubierto informático. Pongámonos en el supuesto en el que este contacta desde un perfil creado en un foro de la “Dark web” con un individuo, del que sabe que forma parte de un grupo de WhatsApp en el que hay indicios de que se comparten archivos que contienen pornografía infantil. Todavía no ha invadido su intimidad, ya que se trata de un mero intento de comunicación, a través de internet, en el que no se ha producido ninguna infiltración, ni se conoce dato privado alguno de la vida íntima de aquel con quien se contacta.

Ahora bien, desde que el agente encubierto informático penetra, siguiendo el ejemplo anterior en el grupo de WhatsApp y, efectivamente, consigue infiltrarse en él, la intimidad de los integrantes del grupo comienza a verse afectada de una manera obvia. La forma de lesionar el derecho a la intimidad no es puntual como puede producirse cuando pinchamos un teléfono, sino que continúa en el tiempo y, por tanto, tiene un carácter duradero⁵⁹. Este aspecto no es algo nimio, ya que implicará que la intimidad de los investigados se vea menoscabada en un mayor nivel.

⁵⁶ STC 25/2019, Sala Primera, de 25 de febrero de 2019, F. J. 4º. El TC reitera que “el derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia de una publicidad no querida, y, en consecuencia, el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido”.

⁵⁷ ZAFRA ESPINOSA DE LOS MONTEROS, R., *El policía infiltrado*, op., cit., p.178. La autora entiende que existen dos momentos en toda infiltración clásica en los que el riesgo de lesión del derecho es diferente. Podemos trasladar esta visión perfectamente a la infiltración del agente encubierto informático.

⁵⁸ ZAFRA ESPINOSA DE LOS MONTEROS, R., *El policía infiltrado*, op., cit., p.180.

⁵⁹ ZAFRA ESPINOSA DE LOS MONTEROS, R., *El policía infiltrado*, op., cit., p.183.

Por ello, la garantía de este derecho se basará en seguir al pie de la letra las actuaciones permitidas en la autorización proporcionada por el juez a la hora de trasladar la identidad ficticia con la que moverse en el mundo virtual, ya que cualquier actuación que sobrepase lo contemplado en la autorización puede generar una responsabilidad en el agente.

Para tratar de evitar que una conducta llevada a cabo por el agente sobrepase la garantía a este derecho, en el caso de que considere indispensable su realización, deberá comunicarse con el juez que emitió el auto autorizando la infiltración para modificar la dispuesto en este y poder ampliar su margen de movimiento, siempre y cuando las actuaciones ampliadas se basen en los principios de proporcionalidad y subsidiariedad, atendiendo a la utilidad y necesidad imprescindibles de la acción.

Cabe poner de manifiesto que la justificación abstracta que legitima al juez autorizar la intervención del agente encubierto informático va más allá. Es, a fin de cuentas, la intención de mantener una seguridad nacional, para lo cual se busca la contención del delito⁶⁰.

1.2.2 Garantía al derecho fundamental al secreto de las comunicaciones

El derecho al secreto de las comunicaciones es un derecho fundamental que aparece contemplado en el art. 18 apartado tercero de la CE. Este implica la garantía que tenemos en torno a que un tercero no pueda acceder a cualquier comunicación que podamos mantener con otra persona.

Como ya hemos comentado la función del agente encubierto informático se basa en mantener comunicaciones en canales cerrados de comunicación, lo que en sí mismo afecta a este derecho⁶¹. De tal forma, que, cabría pensar que cualquier contacto previo en un canal cerrado sin autorización viola el secreto de las comunicaciones.

⁶⁰ ORTELLS RAMOS, M., “Exclusividad jurisdiccional para la restricción de derechos fundamentales y ámbitos vedados a la injerencia jurisdiccional”, *Medidas restrictivas de derechos fundamentales*, CGPJ, Madrid, 1996, p. 20.

⁶¹ Art. 282 bis apartado sexto de la LECrim.

Sin embargo, cabe una excepción admitida por el Alto Tribunal en sus SSTS 767/2007, 752/2010 y 173/2018⁶². Esta se produce en los supuestos a los que se produce la actuación de los *ciber agentes*, que no agentes encubiertos informáticos y que yo mismo denominé con anterioridad ya que creo que puede entenderse mejor como aquellos que realizan “patrullaje cibernético”. Es decir, cuando un agente se encuentra realizando sus funciones de prevención por Internet, y de forma casual, es partícipe de la comisión de un delito como puede ser el envío de fotos de un individuo al propio agente, no será necesaria la autorización para la infiltración, siempre que el propio agente, una vez tenga conocimiento del hecho, pida esta al juez⁶³.

Por tanto, para que un agente encubierto informático inicie la comunicación en un canal cerrado, el TS expone la obligación por parte del juez de atender a la aparición de indicios que vayan más allá de sospechas policiales, evaluando la gravedad del delito y esa necesidad que requiere el principio de proporcionalidad a la hora de tratar con un derecho fundamental⁶⁴.

1.2.3 Garantía al derecho fundamental a la defensa

El derecho al secreto de las comunicaciones es un derecho fundamental que aparece contemplado en el art. 24 apartado segundo de la CE, donde, entre otros, se encuentran el derecho a no declarar contra sí mismo y a no confesarse culpable, los cuales pueden verse afectados con la actividad de la infiltración y el posterior testimonio de los agentes como derechos públicos constitucionales que toda persona física atesora cuando se le acusa de cometer un hecho delictivo⁶⁵. De hecho, el TC lo ha considerado como una de las garantías más primordiales de un Estado Social y Democrático de Derecho⁶⁶.

De tal manera, que el investigado por parte del agente no está siendo informado al momento de la infiltración, lo que podría llevarnos a pensar que lo obtenido en las

⁶² STS 767/2007, Sala II, Sección 1ª, de 3 de octubre de 2007, F. J. 4º. STS 752/2010, Sala II, Sección 1ª, de 14 de julio de 2010, F. J. 1º y STS 173/2018, Sala II, Sección 1ª, de 11 de abril de 2018, F. J. 7º.

⁶³ LAFONT NICUESA, L., *El agente policial encubierto*, Tirant lo Blanch, Valencia, 2022, p. 444.

⁶⁴ STS 13 de marzo 2019, F. J. 2º.

⁶⁵ GIMENO SENDRA, J. V., “El derecho de defensa”, *Constitución y proceso*, Tecnos, Madrid, 1988, p. 88.

⁶⁶ STC 229/1999, Sala Primera, de 13 de diciembre de 1999, F. J. 2º.

conversaciones dentro de los canales cerrados de comunicación carece de valor probatorio.

No obstante, la tesis aceptada en España respecto a ello se basa en el argumento de que, al no ser un interrogatorio como tal, el agente no tiene ese deber de información, lo que se puede considerar como la notificación tardía de sus derechos una vez se levanta el secreto de sumario. Eso sí, siempre respetando los demás principios probatorios en lo que pueda referirse a posibles grabaciones u otras formas de obtener las fuentes de prueba. Ello se sustenta en la identidad ficticia que dota al juez al agente encubierto informático, ya que legitima que el infiltrado y el presunto delincuente mantengan una conversación donde el primero averigua elementos trascendentales para la investigación. Así, si la comunicación mantenida es libre y consentida por el delincuente, podemos considerarlo como si se tratara de una autoincriminación⁶⁷.

2. Forma de proceder en la fase de investigación y actuaciones que puede llevar a cabo

Como ya hemos venido haciendo referencia a lo largo del capítulo, la intervención por parte del agente encubierto en la fase de instrucción se basará en intentar obtener todas las pruebas posibles mediante las actuaciones a las que nos vamos a referir en este apartado, además de las que comparte de manera general con el agente encubierto clásico.

Todas estas acciones deberán preverse en el auto de autorización emitido por el juez, para garantizar el respeto de los DDFF de los investigados, los cuales son más fácilmente lesionables que en otro tipo de diligencias, además de verse afectados un mayor número de ellos.

Una vez que conocemos cómo debe actuar el agente encubierto informático y las limitaciones que debe acatar, es importante valorar su participación como testigo ante el juez de instrucción. La doctrina de forma mayoritaria concuerda que, para el caso del agente encubierto clásico su comparecencia para testificar en el juzgado de instrucción puede suponer un gran peligro para su integridad. Asimismo, no resulta necesario que

⁶⁷ ZAFRA ESPINOSA DE LOS MONTEROS, R., *El policía infiltrado*, op., cit., p.214 y 216.

acuda, ya que las pruebas obtenidas gracias a las actuaciones que haya llevado a cabo infiltrado bajo la identidad supuesta pueden ser conservadas en una pieza separada para utilizarse posteriormente en el proceso⁶⁸.

En mi opinión, ello puede ser trasladable al ámbito del agente encubierto informático. Es cierto, que los investigados no conocen la apariencia física del infiltrado, lo que, quizá, puede implicar que el peligro al que se exponga el agente encubierto informático sea menor, aunque en ningún caso descartable.

Sin embargo, el testimonio del agente en esta fase mediante su presencia en el juzgado de instrucción puede poner en riesgo la investigación, ya que puede generar una alarma entre los presuntos delincuentes, en el caso de que se hagan con la información de lo dicho. Tengamos en cuenta que se estarían aportando datos que solo una persona infiltrada conocería. De ahí, que por la posible presencia de un “topo” en su canal de comunicación, pasasen a actuar de forma más cauta, tratando de eliminar posibles pruebas e, incluso, trasladando el foro a otro lugar de la Dark Web.

Una vez visualizado de manera general al agente en esta fase, vamos a contemplar las actuaciones que durante este período puede llevar a cabo. El agente encubierto informático comparte muchas de las actuaciones que la figura clásica realiza en la fase de investigación de un supuesto delito, por ejemplo, el deber de informar al juez de sus actuaciones o el empleo de sistemas de escucha o videovigilancia⁶⁹. Eso sí, muchos autores llevan años aduciendo a una falta de referencias en el ordenamiento que permitan extraer competencias concretas de este agente⁷⁰. No obstante, a partir de la naturaleza virtual de este agente y con ayuda de lo poco que establece el art. 282 bis LECrim apartado sexto podemos tratar ciertas actuaciones específicas y propias.

2.1 Crear un perfil en un foro y conversar en él autorizado bajo identidad ficticia

⁶⁸ MARTÍNEZ QUIROGA, J.F., “Entrada y registro, entregas vigiladas, apertura de paquetes y postales, agente encubierto y figuras afines”, curso de formación continua de fiscales *La investigación en el delito de tráfico de drogas y su incidencia en el juicio oral*, Centro de Estudios Jurídicos, 2015, p. 31.

⁶⁹ El art. 282 bis apartado séptimo expone que el agente encubierto informático, previa autorización del juez, podrá “obtener imágenes y la grabar 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.

⁷⁰ BUENO DE MATA, F., *Las diligencias de investigación penal...*, op., cit., p.114.

Ello supone la función principal del agente en esta fase de indagación, como así establece el propio art. 282 bis apartado sexto. Es decir, el agente tendrá libertad para actuar en estos foros, que la ley reconoce como canales cerrados de comunicación, siempre que en la autorización otorgada por el juez se le dé acceso a ello.

Para ello, está legitimado a crear un perfil falso. Cuando deba rellenar los distintos campos hasta tener la cuenta del foro, será necesario que utilice los datos que se le hayan sido entregados en torno a su identidad ficticia⁷¹, no solo en lo relativo a su nombre, sino también aquellos referentes a la edad, número de identificación o cualquier otro indispensable para obtener la cuenta.

Así, podemos entender esta función como paralela a la participación en el tráfico jurídico y social bajo identidad supuesta a la que se refiere DEL POZO PÉREZ, M.⁷² para el agente encubierto físico.

2.2 Abrir cuentas corrientes y comerciar electrónicamente

Para dotar de verosimilitud a la identidad supuesta que defiende el agente encubierto económico y, a la vez, poder realizar transacciones que puedan servir de prueba en la fase de enjuiciamiento, el juez podrá autorizar la creación de cuentas que doten de dinero al agente y le permitan operar sobre el objeto ilícito al que se esté enfrentando.

Todo esto servirá de gran utilidad para grandes estafas cibernéticas realizadas por organizaciones criminales. Además, cabrá la posibilidad que el dinero utilizado por el agente tome la forma de criptomoneda⁷³, algo que considero, es esencial, debido a que las organizaciones criminales realizan sus negocios a través de estas monedas digitales, ya que con su uso no se les puede seguir el rastro.

⁷¹ BUENO DE MATA, F., *Las diligencias de investigación penal...*, op., cit., p. 118.

⁷² DEL POZO PÉREZ, M., “El agente encubierto como medio de investigación...”, op., cit., p. 298.

⁷³ CLADERA ALBA, F., y GARCÍA MARTÍNEZ, G., “Blanqueo de capitales y agente encubierto en Internet” en BUENO DE MATA, F., (coord.), *Fodertics 5.0. Estudios sobre nuevas tecnologías y justicia*, Editorial Comares, 2016, p.199. Citado por LAFONT NICUESA, L. en *El agente policial encubierto*, op., cit., p. 453.

2.3 Acceso a teléfonos asociados a las direcciones de IP

Esta acción no es presupuesto inicial del cometido del agente encubierto informático, porque en la primera autorización que proporcione el juez, no podrá llevarla a cabo. Esto es así, ya que, con anterioridad al acceso a teléfonos, deberá disponer de los indicios suficientes en torno a la investigación del delito que permitan al juez ampliar las competencias del agente. Hemos de tener en cuenta que se estará viendo afectado el derecho fundamental a la intimidad y, para garantizarlo, como vimos, el juez deberá motivar suficientemente, para ampliar el auto, las razones por las que es necesario realizar esta acción⁷⁴, no pudiendo, por ello, aparecer en el auto original.

2.4 Entrega de archivos que contengan material delictivo

Otra de las actuaciones que contempla el art. 282 bis apartado sexto, párrafo segundo es este intercambio de archivos ilícitos, que tanto debate genera, debido a que puede afectar no solo al derecho de terceras personas, sino que genera una discusión ética perfectamente entendible, y, en algunos casos, podemos hablar de que estos envíos se encuentran cercanos a una provocación e inducción delictiva⁷⁵. De todo ello hablaremos en mayor profundidad cuando nos refiramos a la pornografía infantil en el capítulo tres.

La sutileza de este aspecto al afectar a elementos tan sensibles obliga a que el juez elabore una autorización especial para esta situación, clarificando exactamente los pasos que puede dar respecto a esto el agente.

2.5 Interacción de la infiltración informática con el mundo físico

Es común en la realidad de estas investigaciones que, en razón de la falta de confianza que puedan poseer los investigados ante la aparición de personas ajenas a su círculo, traten de trasladar la relación al mundo físico, es decir, un encuentro en persona, o a conversaciones telefónicas⁷⁶.

⁷⁴ ZAFRA ESPINOSA DE LOS MONTEROS, R., *El policía infiltrado*, op., cit., p.183.

⁷⁵ BUENO DE MATA, F., “El agente encubierto en Internet... op., cit., p. 304.

⁷⁶ LAFONT NICUESA, L., *El agente policial encubierto*, op., cit., p. 462 y 463.

En torno al paso de la investigación a la realidad física, LAFONT NICUESA entiende que “será necesaria una nueva autorización únicamente si se activa un agente físico para acudir a dicha reunión⁷⁷”. Parece lógico, sobre todo después de haber desgranado los presupuestos que llevan a un agente a poder realizar funciones encubiertas físicas o informáticas, que el agente encubierto informático que ha llevado la infiltración por esta vía, no será la persona propicia para continuar la infiltración en el mundo físico, debido a que las condiciones que han de tener uno y otro no son las mismas⁷⁸. Por ello, el juez deberá confeccionar una nueva autorización designando un agente encubierto físico para que siga investigando.

3. Intervención del agente en la fase de juicio oral

Existe cierta confusión en torno al hecho de que muchas personas creen que la propia infiltración realizada por el agente encubierto informático es prueba en sí misma tenida en cuenta en el juicio oral. Pero recordemos que es una diligencia de investigación que sirve como forma de obtención de los medios de prueba, que serán los que introduzcamos en el proceso, en la fase del juicio oral, para ser tomados en cuenta por el juez decisor con el fin de dictar sentencia. La problemática se sitúa, por ende, en ver qué medios de prueba podemos utilizar en el acto del juicio oral.⁷⁹

El agente encubierto informático, como regla general, deberá declarar como testigo y ratificar lo dispuesto a modo de prueba documental. Es considerado su testimonio, en la mayoría de los supuestos donde se da, como prueba principal e, incluso, en ocasiones, ha servido como prueba de cargo. No obstante, aunque la declaración sea la prueba a tener más en cuenta, no debería servir en exclusividad para romper el principio de presunción de inocencia. Sino que lo conveniente es que, junto a ella, se tengan en cuenta pruebas complementarias que refuercen y secunden esta prueba principal⁸⁰.

De esta forma, si unimos a la prueba testifical del agente, el testimonio de los acusados (donde la falta de convicción de sus argumentos dotará de razón a lo dicho por el agente),

⁷⁷ LAFONT NICUESA, L., *El agente policial encubierto*, op., cit., p. 462.

⁷⁸ BUENO DE MATA, F., *Las diligencias de investigación penal...* op., cit., p. 116.

⁷⁹ ZARAGOZA TEJADA, J.I., “La modificación operada por la Ley 13/2015. El agente encubierto informático”, en FERNÁNDEZ BERMEJO, D. (coord.), y SANZ DELGADO E. (coord.), *Tratado de Delincuencia Cibernética*, Aranzadi, Navarra, p. 29.

⁸⁰ LAFONT NICUESA, L., *El agente policial encubierto*, op., cit., p. 471.

las diversas capturas de conversiones o transferencias de dinero aportadas como prueba documental y la reproducción de grabaciones telefónicas o de vídeos enviados por los acusados al agente, tendremos argumentos suficientes para quebrar la presunción de inocencia de estos.

Recordemos que, para todo ello, el agente encubierto informático, como constatación de que no ha existido una provocación del delito mantendrá, a menos que decida acogerse al programa de testigos protegidos, su identidad ficticia en el acto del juicio oral⁸¹.

Es importante, en último lugar, hacer una referencia a la distinción existente entre el agente encubierto clásico e informático en esta fase del proceso. Desde mi punto de vista, la declaración del agente encubierto informático denota una convicción mayor, puesto que su condición de experto en informática le lleva a una posición casi mixta entre testigo y perito.

Conviene desarrollar esta idea dada su trascendencia. La declaración testifical⁸² y el informe pericial⁸³ son medios de prueba a través de los cuales introducimos las fuentes de prueba en el proceso, pero sus funciones en el seno de este son diferentes.

A través del informe pericial, se incluyen en el proceso conocimientos especializados referentes a la multiplicidad de ámbitos diferentes a tratar para solventar un caso. No podemos esperar que los operadores jurídicos dispongan de las competencias de un experto, ya que eso no es posible⁸⁴. Mientras que la declaración testifical supone que una persona que conozca ciertos hechos los exponga, debido a su presencia en ellos o porque ha recibido una versión de estos,⁸⁵.

Con el agente encubierto físico parece claro que, el papel que puede tomar en fase de juicio oral es el de aportar como testigo aquello que ha presenciado como parte de su infiltración dentro del grupo de criminalidad organizada.

⁸¹ Art. 282 bis, apartado segundo.

⁸² Capítulo V, Título V, Libro II LECrima, arts. 410 a 450.

⁸³ Capítulo VII, Título V, Libro II LECrim, arts. 456 a 485.

⁸⁴ ABEL LLUCH, X., “La prueba pericial”, *Colección de formación continua Facultad de Derecho ESADE, Serie de estudios prácticos sobre los medios de prueba*, en GINÉS CASTELLET, N., (coord.), Bosch Editor, 2009, p. 16.

⁸⁵ STS 1124/1995, Sala II, Sección 1ª, de 15 de diciembre de 1995, F.J. 2º.

Ahora bien, si atendemos al agente encubierto informático, su función a tenor de las preguntas de las partes y las aclaraciones que precise el propio juez, podrá traspasar lo relativo a aquello acontecido en el seno del canal cerrado de comunicación e iluminar a los presentes en el juicio oral acerca de cuestiones informáticas, difícilmente conocibles por alguien sin conocimientos informáticos, pero de especial trascendencia para la resolución y sobre todo motivación de la sentencia, tales como la explicación del funcionamiento de foros en la *Dark web*, la rareza de su acceso por medio de navegadores y motores de búsqueda distintos a los utilizados en el Internet visible, o la utilización como medio de pago de monedas digitales para perder el rastro que puedan dejar los delincuentes, todos ellos ya referenciados con anterioridad.

Al final todo nos hace retornar, en primer lugar, a las diferencias de cualificación entre ambos agentes encubiertos y, de esta forma, es como más claro podemos comprobar que la infiltración requiere unas características psíquicas y emocionales mínimas, además de ciertos conocimientos jurídicos y de seguridad, pero la exigencia de ese *plus* de conocimientos en informática no proviene solo por tratarse del medio en el que se lleva a cabo la infiltración. Realmente, puede determinar en un proceso la diferencia, o no, de que un juez comprenda y reconozca lo verdaderamente acontecido en un ámbito tan lejano como puede ser la informática para él, y ello le permita quebrar la presunción de inocencia de los investigados con una exposición exacta de los hechos probados y la correspondiente motivación jurídica.

Y, en segundo lugar, a comprobar que el propio precepto legal en el art. 282 bis apartado sexto, párrafo segundo *in fine*, dota al agente encubierto informático de la capacidad de “analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos”, lo que supone una tarea que un mero testigo referenciador de los hechos no podría llevar a buen puerto, sino solo un verdadero experto en informática.

CAPÍTULO 3: ESPECIAL REFERENCIA AL AGENTE ENCUBIERTO INFORMÁTICO EN CASOS DE GROOMING Y PORNOGRAFÍA INFANTIL

1. Concepto de grooming, su relación con la pornografía infantil y el papel de las nuevas tecnologías en ellos

Como ya hemos ido mostrando a lo largo del trabajo, la tecnología y, en concreto la aparición de Internet y, posteriormente de las redes sociales ha supuesto un enorme cambio en la vida de las personas. Para muchos, el cambio ha dado lugar a una mejora en su día a día. Tanto en el trabajo, como en el ocio los beneficios han sido incontables. Sin embargo, para muchos otros, esta alteración ha supuesto un infierno, ya que es el perfecto escenario para que los delincuentes sexuales den rienda suelta a sus más oscuras filias. Ya no tienen que acudir a parques de juegos o a los alrededores de los colegios, sino que desde el sofá de su casa pueden conectarse dentro del mismo territorio donde, desprotegidas, se relacionan sus víctimas.

El problema del ordenamiento jurídico penal para combatir estos comportamientos residía y, todavía en algunos aspectos, a día de hoy, reside en que este estaba pensado para combatir delincuentes individuales en el mundo físico y no para perseguir acciones delictivas a través de Internet⁸⁶. Más aún si los delitos venían cometidos por grupos de criminalidad organizada. De ahí que la realidad político-criminal precisaba una evolución en el Derecho Penal, sin dejar de lado los cimientos sobre los que se sustenta, tales como los principios o garantías de DDFF vistos.

En este contexto es donde surge la acción del llamado *grooming*. El significado literal del verbo *to groom* es acicalarse en castellano. Si enmarcamos este verbo en la expresión “acicalar a alguien para algo” podemos comenzar a hacernos una idea del porqué de la generalización de este término y a lo que se quiere hacer referencia con ello.

En relación a ello, GUDÍN RODRÍGUEZ-MAGARIÑOS inicia una aproximación a esta expresión, argumentando que se basa en que una persona se oculta con la intención

⁸⁶ CRUZ DE PABLO, J. A. *Derecho Penal y nuevas tecnologías: aspectos sustantivos*, Difusión Jurídica, Barcelona, 2006.

de dar inicio a una seducción en la que trata de captar la voluntad de un menor, la cual se encuentra en proceso de formación⁸⁷.

En función de lo anterior, podemos obtener una definición ya completa marcada por RAMOS VÁZQUEZ, quien entiende que el concepto de grooming implica “un proceso gradual mediante el que una persona establece una relación de confianza con menores, relación enmascarada como de amistad, en la que abundan los regalos y las muestras de atención y afecto y que, gradualmente, deriva en un contenido sexual en un modo que resulta natural y no intimidatorio para el propio menor⁸⁸”

Muchos suelen errar al considerar el grooming o, delito de *child grooming*, un acoso sexual por parte de un adulto hacia un menor de edad. En nuestro ordenamiento jurídico el acoso sexual se describe como una situación, en la que, mediando relación laboral o docente previa, se solicitan favores de naturaleza sexual. Ello no es aplicable al caso, porque no partimos de que se produzca una de esas relaciones con anterioridad, ni se requiere una continuación en la conducta⁸⁹ (el grooming comienza desde el primer contacto). Partimos solo de una intención de establecer una relación y control emocional sobre un menor de edad⁹⁰

Por tanto, debemos desterrar esta idea equivocada de nuestras cabezas y entender desde la visión del delito actual de grooming del art. 183 ter CP, que este hecho delictivo consiste en ese contacto previo dirigido a la perpetración de otra figura delictiva, a través de una proposición de un encuentro físico (apartado primero del art. 183 ter CP) o para conseguir que el menor le mande material pornográfico (apartado segundo del art. 183 ter CP). Es decir, es un delito que sirve como medio para cometer otros delitos de carácter sexual⁹¹

⁸⁷ GUDÍN RODRÍGUEZ-MAGARIÑOS, F., “Algunas consideraciones sobre el nuevo delito de grooming”, *Delincuencia informática. Tiempos de cautela y amparo*, Thomson Reuters, Navarra, 2012, p. 142.

⁸⁸ RAMOS VÁZQUEZ, J. A., “El llamado delito de “child grooming”: consideraciones acerca del nuevo artículo 183 bis del Código Penal”, disponible en <https://bit.ly/3bg4NM4>, (consulta 14-05-2022).

⁸⁹ Art. 184.1 CP.

⁹⁰ STS 97/2015, Sala II, Sección 1ª, de 24 de febrero de 2015, F. J. 1º.

⁹¹ DÍAZ CORTÉS, L. M., “El denominado “child grooming” del artículo 183 bis del Código Penal: una aproximación a su estudio”, *Boletín del Ministerio de Justicia*, disponible en: <https://bit.ly/3n7fuTT>, (consulta 14-05-2022).

Su carácter de puente hacia otras conductas es lo que dota al grooming de esa peligrosidad, lo que obliga al legislador a prevenir estos comportamientos para evitar la posterior comisión de delitos más graves, como el abuso sexual o la divulgación o tenencia de material pornográfico infantil, entre otros. Así lo entienden GONZÁLEZ ALONSO Y DE CASTRO HERNÁNDEZ “se aprovechan de la vulnerabilidad del menor para obtener beneficios personales de tipo pornográfico o sexual”⁹².

Nosotros vamos a centrarnos en el paso del grooming a la posible facilitación de material pornográfico del art. 183 ter apartado segundo CP, conocido ampliamente bajo el término *sexting*. Esta voluntad de obtener tal material constituye el elemento subjetivo del tipo, es decir, la intención del contacto vía Internet tiene como finalidad embaucar al menor para conseguir fotos y vídeos de este. No se exige que, efectivamente, se dé el resultado de recibir el material. El delito de sexting del art. 183 ter apartado segundo se perfecciona con el mero contacto. De tal manera que, si se llegase a recibir este de un menor de 16 años, estaríamos ante un concurso entre las conductas contempladas en el art. 183 ter apartado segundo y el art. 189 CP⁹³.

Con la remisión a este art. 189 CP, en el que se regulan multitud de actuaciones que resultan en la comisión de delito, existe una controversia, puesto que el delito de sexting del art. 183 ter apartado segundo fue incorporado tras la firma del Convenio de Lanzarote⁹⁴. Es en su art. 23 donde, en remisión al art. 20 se nos enumeran los “delitos relativos a la pornografía infantil. La enumeración realizada en él difiere de todos los comportamientos considerados como delito relativo a la pornografía infantil del art. 189. CP, ya que aquí se incluyen actuaciones como la captación de menores para espectáculos exhibicionistas y la financiación para actividades pornográficas de menores que no aparecen en el art. 20 del Convenio de Lanzarote.

Considero, por tanto, que el legislador debería aclarar este conflicto legislativo y adaptar la remisión del art. 183 ter apartado segundo CP hacia el art. 189 CP en unos

⁹² GONZÁLEZ ALONSO, F., DE CASTRO HERNÁNDEZ, R. M., *Mejorar la convivencia. Educación en valores y Derecho Educativo*, Tirant Humanidades, Valencia, 2019, p. 125.

⁹³ SAINZ-CANTERO CAPARRÓS, J. E., “Delitos contra la libertad e indemnidad sexuales (I)”, *Sistema de Derecho Penal. Parte Especial*, Dykinson, Madrid, 2016, p. 261.

⁹⁴ Convenio del Consejo de Europa para la protección de lo niños contra la explotación y el abuso sexual, hecho en Lanzarote el 25 de octubre de 2007. Ratificado por España el 12 de marzo de 2009. *BOE* núm 274/2010, pp. 94858 a 94879.

términos donde no se entienda ampliada la lista de delitos relativos a la pornografía infantil, con respecto a lo que dicta el instrumento supranacional, el cual debe prevalecer.

Visto el concepto de grooming y su relación con la pornografía infantil, debemos abordar para finalizar la comprensión de este apartado el papel del consentimiento del menor en este aspecto.

Tras la LO 1/2015 de reforma del CP⁹⁵ (en adelante, LO 1/2015), la edad para poder dar el consentimiento sexual aumentó de lo 13 a los 16 años. Así lo contempla el tipo objetivo del 183 ter CP “El que... contacte con un menor de 16 años”. Sin embargo, cabe una excepción y es la prevista en el art 183 quater CP, donde podemos encontrarnos una excusa absolutoria de la responsabilidad penal para los delitos situados en el Capítulo de los abusos sexuales “cuando el autor sea una persona próxima al menor por edad y grado de desarrollo o madurez física y psicológica”.

A esta excepción se ha referido el Tribunal Superior de Justicia de Castilla y León (TSJCyL) en el conocido como “caso Arandina” en el que a uno de los autores se le absolvió aplicando este artículo. En el supuesto el Tribunal expone que para que opere este precepto “se hace preciso indagar si existe una simetría de edad /grado de madurez y desarrollo entre la menor y los adultos”⁹⁶

En consecuencia, será un elemento a tener muy en cuenta cuando estemos ante cualquier situación en la que, presumiblemente, exista la posibilidad de aplicar el precepto.

2. Regulación de ambas figuras

El pavor que produjo el aumento de la ciberdelincuencia en el seno de la UE y el Consejo de Europa fue motivo para que España comenzase a ratificar instrumentos supranacionales para tratar de frenarla.

⁹⁵ Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 1/1995, de 23 de noviembre, del Código Penal.

⁹⁶ STSJCyL 14/2020, Sala de lo Civil y Penal, de 18 de marzo de 2020, F. J. 12º.

El antecedente más lejano en el que se ofrece un primer significado de pornografía infantil se sitúa en el art. 9.2 del Convenio sobre la Ciberdelincuencia del año 2001⁹⁷. Tras este apareció la Decisión Marco 2004/68/JAI del Consejo⁹⁸, en la que se referencia la conducta del adulto por la cual ofrece al menor un pago (sea de la índole que sea) en contraprestación por la práctica de relaciones sexuales. Este instrumento ha sido criticado por la doctrina la cual entiende que la aplicación práctica de la Decisión viene muy dificultada al tener una condición exageradamente extensa⁹⁹.

Ahora bien, el Convenio que más hizo evolucionar nuestro ordenamiento y en el que, se hace ya una apreciación directa al delito de grooming y la variante del sexting, es el ya mencionado Convenio de Lanzarote de 2007. En él, en su art. 23, se obliga a los firmantes a “adoptar las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito el hecho de que un adulto, mediante las tecnologías de la información y la comunicación, proponga un encuentro a un niño que no haya alcanzado la edad de 16 años con el propósito de cometer un delito de abuso sexual o delitos de pornografía infantil”. La ratificación de este Convenio por parte de España implicó la necesidad de reformar el CP para tipificar este delito.

Así las cosas, se elaboró la Ley Orgánica 5/2010¹⁰⁰ (en adelante, LO 5/2010), donde se incluyó el art. 183 bis CP. En él se recogió, por primera vez, el delito de grooming. A diferencia con la regulación actual que aparece en art. 183 ter, este artículo tenía, únicamente, un párrafo. La conducta castigada era similar a la actual. Condensaba en un apartado ese contacto y posterior propuesta para “concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189”, es decir, para un subsiguiente abuso sexual o delito de pornografía infantil. La diferencia más relevante, además de la diferenciación penológica, se da en el aumento de edad del consentimiento, que como ya dijimos, se incrementó de los 13 años en esta ley, a los 16 en el CP actual.

⁹⁷ Convenio del Consejo de Europa sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Ratificado por España el 23 de noviembre de 2001, *BOE* núm. 226/2010, pp. 78847 a 78896.

⁹⁸ Decisión marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil. *DOUE* núm 13/2004, pp. 44 a 48.

⁹⁹ CUERVO NIETO, C., “El delito de child grooming en el Derecho Penal español. Análisis del tipo penal y breves reflexiones”, disponible en <https://bit.ly/3n8fTp2>, (consulta 15-05-2022).

¹⁰⁰ Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre de Código Penal.

Ahora bien, el legislador en la exposición de motivos de la LO 5/2010, expuso que la confección de esta ley se debió a la adaptación obligatoria de la Decisión Marco 2004/68/JAI, sin hacer referencia al Convenio de Lanzarote¹⁰¹ o al Protocolo Facultativo de la Convención sobre los Derechos del Niño¹⁰², debiendo ser citados al formar parte de nuestro ordenamiento jurídico interno y hacer referencia a la pornografía infantil¹⁰³

Un año después de la reforma del CP en 2010, desde la UE se elaboró la Directiva 2011/93/UE del Parlamento y el Consejo¹⁰⁴, con la intención de alcanzar el objetivo no conseguido por la Decisión Marco 2004/68/JAI, lograr un marco jurídico general aplicado y traspuesto por todos los Estados, en torno a la explotación sexual de menores y pornográfica infantil¹⁰⁵.

De ahí, llegamos a la ya conocida LO 1/2015, la cual tipificó en el art. 183 ter el delito de grooming. Esta elevó, como sabemos, la edad de consentimiento sexual a los 16 años y creó el delito de sexting en el 183 ter apartado segundo que tanto nos interesa para el estudio de este trabajo.

3. Modo de actuación por el agente encubierto

Antes de comenzar a exponer el modo de actuación del agente encubierto informático, debemos situar cronológicamente cuál es el momento en el que debe adoptarse esta medida.

¹⁰¹ SÁNCHEZ ESCRIBANO, M. I., “Reflexiones sobre el child grooming. A propósito del libro *El delito de online child grooming o propuesta sexual telemática a menores*”, *Revista Jurídica de las Islas Baleares*, núm. 15, 2017, p. 20.

¹⁰² Instrumento de Ratificación del Protocolo Facultativo de la Convención sobre los Derechos del Niño, relativo a la venta de niños, prostitución infantil y la utilización de niños en la pornografía, hecho en Nueva York el 25 de mayo del 2000. Ratificado por España el 5 de diciembre de 2001, *BOE* núm. 27/2002, pp. 3917 a 3921.

¹⁰³ DOLZ LAGO, M. J., “Child grooming y sexting: anglicismos, sexo y menores en el Código Penal tras la reforma del 2015”, *Diario la Ley*, disponible en <https://bit.ly/3Qxsks9>, (consulta 16-05-2022), Madrid, 2016.

¹⁰⁴ Directiva 2011/93/UE del Parlamento y el Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, *DOUE* núm. 335/2011, pp. 1 a 14.

¹⁰⁵ Exposición de motivos de la Directiva 2011/93/UE del Parlamento y el Consejo, de 13 de diciembre de 2011, apartado (6).

El inicio de las gestiones para adoptar la infiltración, en la práctica, suele darse a partir de que el menor manifieste, de alguna forma, que está ocurriendo algo que le hace encontrarse aterrado y con un sentimiento de culpa o sus progenitores noten un cambio relevante en su carácter¹⁰⁶.

Esto provoca que, cuando los padres toman la iniciativa de denunciar, casi todos los casos se encuentran en una fase avanzada en la que el menor ya ha entregado algún archivo delicado al adulto o, incluso, ha existido ya un encuentro en el mundo real. Parece complicado pillar la conducta en una etapa anterior, aunque sería lo más ideal. Realmente, es cuando se produce el delito de grooming, (el contacto con intención de un encuentro posterior) o el de sexting, donde la intención del contacto va dirigida a obtener el material pornográfico.

En mi opinión, esto ocurre de esta manera, ya que un menor de 16 años, generalmente, y sin atender a los supuestos en el que este alberga una madurez avanzada¹⁰⁷, no tiene la capacidad ni la experiencia para entender que el contacto que está llevando a cabo el mayor de edad viene justificado por esas dos intenciones y no por cualquiera de las razones que le pueda estar dando el autor del delito. O que, detrás de una mera solicitud de amistad de quien parece ser un menor como él o alguien que puede gustarle, se esconde una persona cuyas expectativas no son las que él cree que tiene.

De tal manera que, los progenitores no tienen forma alguna de darse cuenta del inicio de este contacto, hasta que acontece alguno de los supuestos más graves, momento en el cual el menor pasa a ser consciente de lo que está ocurriendo y, es ahí, cuando los padres tienen la opción de notarlo.

Por todo ello, es difícil que pueda existir la adopción de la medida del agente encubierto informático o cualquier otra menos lesiva en este período previo, ya que, es prácticamente imposible constatar la existencia de un posible delito que legitime la

¹⁰⁶ PANIZO GALENCE, V., “el ciber-acoso con intención sexual y el child-grooming”, *Quadernos de criminología: revista de criminología y ciencias forenses*, núm. 15, 2011, p. 27.

¹⁰⁷ Eso sí, la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales entiende que un menor alberga, con carácter general, la madurez suficiente para consentir el trato de sus datos en redes sociales con catorce años en su artículo 7.

adaptación de esta figura¹⁰⁸. Al final, estos contactos previos han de tratar de ser interceptados por los agentes que se encarguen de realizar el patrullaje cibernético, cuyo grupo más conveniente para tomar esta función como suya es la Brigada de Investigación Tecnológica de la Policía Judicial¹⁰⁹. Al igual que, pienso que será esencial una correcta prevención de los padres para evitar estas circunstancias, basándose en una educación digital y la siembra de una relación de confianza que permita conocer una situación así desde el principio.

En vista de que, hemos previsto el momento a partir del cual aparece la figura del agente encubierto informático, es ahora momento de centrarnos en su modo de actuación en sí.

Desde que la utilización de las redes *peer to peer* perdieron popularidad en detrimento de canales cerrados de comunicación en foros de la *Dark Web*¹¹⁰, la actuación de los de los agentes encargados del patrullaje informático perdió todo el sentido y pasó a ser ineludible la aplicación de una medida que posibilite acceder a estos canales donde se intercambian archivos pornográficos de menores de edad, el agente encubierto informático.

Conviene recordar, que aparte de poder tratar los delitos de criminalidad organizada del art. 282 bis apartado cuarto LECrim, el ámbito objetivo del agente encubierto informático se amplía a los delitos que contempla el art. 588 ter a LECrim. Este nos remite a los delitos que contempla el art. 579.1 LECrim, entre los que encontramos los delitos relativos a la pornografía infantil, estén hechos por un grupo de criminalidad organizada o no.

Para aquello que tiene que ver con la lucha contra la pornografía infantil, será importantísimo y muy controvertido el intercambio o envío por sí mismo de archivos ilícitos por razón de su contenido¹¹¹, para el cual está legitimado el agente encubierto

¹⁰⁸ Recordemos lo relativo al principio de proporcionalidad, subsidiariedad y especialidad.

¹⁰⁹ BUENO DE MATA, F., “El agente encubierto en internet...”, op., cit., p. 301.

¹¹⁰ CAROU GARCÍA, S. “El agente encubierto como instrumento de lucha contra la pornografía infantil en internet. El guardián al otro lado del espejo”, *Cuadernos de la Guardia Civil: Revista de seguridad pública*, núm. 56, 2018, p. 27.

¹¹¹ Art. 282 bis LECrim, apartado sexto, párrafo segundo.

informático, siempre con autorización específica del juez, diferente a la que le dota de identidad supuesta para comenzar su actividad como agente encubierto informático.

Cuando uno de estos agentes, tras mucho trabajo, es capaz de ganarse la confianza de al menos uno de los integrantes del canal cerrado de comunicación y logra entrar en él, es muy común que los demás participantes del grupo le pidan como prueba “de su buena fe”, que envíe un archivo del material pornográfico de menores que tenga en su colección.

Llegados a este punto, la problemática a la que se ha enfrentado la doctrina es grande. Una entrega controlada de estos archivos informáticos queda fuera de lo recogido en el art. 263 bis LECrim que regula la entrega vigilada¹¹². DEL POZO PÉREZ, M. considera que la regulación de este artículo es escasa e insuficiente¹¹³. De tal manera que estamos ante una entrega controlada que el ordenamiento jurídico procesal-penal no permite.

La falta de regulación de una entrega controlada de este tipo nos hace dudar de la posible implicación en una provocación o inducción del delito por parte del agente encubierto informático y la consecución o duración en el tiempo de la entrega. Además, considero importante reflexionar acerca de si, llevando a cabo el mismo delito que los integrantes del foro se está lesionando el bien jurídico en cuestión (la indemnidad sexual) y sobre todo si se está poniendo en cuestión un principio, que no debe verse afectado por la pretensión de resolver un delito, como es el principio de interés superior del menor por los propios poderes públicos del Estado.

La solución que más comparto a la apreciación de esta problemática es la propuesta por BUENO DE MATA, F. Este, en lugar de acudir a antiguos archivos obtenidos en investigaciones pasadas, propone intercambiar lo que denomina como “material camuflado” donde actores y actrices mayores de edad con apariencia de menores, voluntariamente, simulen aquello que buscan los pedófilos¹¹⁴

¹¹² La entrega vigilada en el art. 263 LECrim aparece regulada para la entrega de drogas tóxicas, sustancias prohibidas, materiales y sustancias del art. 371 CP, bienes y ganancias del 301 CP, y bienes objetos y especies materiales y vegetales de los arts. 332, 334, 386, 399 bis, 566, 568 y 569 CP. No se recoge la entrega informática de elementos de pornografía infantil.

¹¹³ DEL POZO, PÉREZ, M. “La entrega vigilada como medio de investigación de la delincuencia organizada en la Ley de Enjuiciamiento Criminal Española”, *Pensamiento jurídico*, núm. 28, p. 161.

¹¹⁴ BUENO DE MATA, F., “El agente encubierto en internet...”, op., cit., p. 303.

Para evitar que el material aportado por el agente encubierto informático siguiese circulando por diferentes grupos de este ámbito, lo mejor sería incluir en los archivos algún elemento que imposibilitase su reenvío¹¹⁵.

De igual forma, hemos de tratar no dejar rastro sobre dónde procede el archivo. Pienso que debemos intentar algo más que la utilización de un ordenador ajeno a la propiedad del Estado. Puede ser interesante incluir una línea de código falsa¹¹⁶, ya que no debemos olvidar que muchos de estos delincuentes son, también, expertos en informática.

¹¹⁵ BUENO DE MATA, F., “El agente encubierto en internet...”, op., cit., p. 304.

¹¹⁶ CUERVO, V. expone en su web: <https://lineadecodigo.com/linea-de-codigo/que-es-una-linea-de-codigo/>, que una línea de código es una sentencia del lenguaje que permite hacer funcionar un programa. Por tanto, si conseguimos falsear la línea de código estaremos borrando nuestra huella.

CONCLUSIONES

Primera: el agente encubierto y el agente encubierto informático son dos figuras, integrantes de la Policía Judicial, que autorizados por el juez (o el Ministerio Fiscal también en el caso del agente encubierto físico) se infiltran bajo una identidad supuesta de distinta forma. El primero puede investigar delitos cometidos en el seno de la criminalidad organizada, mientras que el ámbito objetivo de actuación del segundo es mayor al poder utilizarse en la indagación, no solo de hechos delictivos cometidos por organizaciones criminales desde Internet, sino también de delitos llevados a cabo por cualquier persona en este medio siempre que se cumplan las características del art. 579.1 LECrim.

Segunda: La infiltración clásica e informática, aunque comparte modos de actuación y objetivos, tienen igualmente diferencias muy marcadas. Si el ordenamiento jurídico hubiese podido contener y resolver la aparición de infinidad de hechos delictivos en Internet con las medidas existentes, el agente encubierto informático no habría sido necesario. Sin embargo, la evolución tecnológica y la adaptación a ella de los potenciales delincuentes, ha obligado a una motorización normativa con la que tratar de combatirlos. Para ello, se elaboró la LO 13/2015. Esta, aunque no lo suficientemente moderna y adaptada a la realidad en continua evolución, introdujo la figura del agente encubierto informático que ayuda al freno de estas situaciones desde la red.

Tercera: La dificultad y peligrosidad de las funciones del agente encubierto, tanto en la versión física como la informática suponen que, no cualquier persona y, ni siquiera cualquier agente pueda desempeñar este cometido. El pertenecer a la Policía Judicial y, además, contar con una serie de características y aptitudes en función del ámbito físico o informático, aparecen como requisito indispensable para que el juez autorice la medida y dote al agente de identidad supuesta. Realmente, están en juego no solo los bienes jurídicos individuales del agente, como su vida o integridad física (principalmente en la modalidad clásica de agente encubierto), sino que también corren peligro bienes jurídicos e intereses colectivos como la correcta administración de justicia. Sin todas estas condiciones, la investigación tendrá menos posibilidades de resultar exitosa y, con ello, muchas personas se seguirán viendo afectadas por esos delincuentes, tanto para el caso investigado en cuestión, como para futuros delitos.

Cuarta: La actuación del agente encubierto informático restringe los DDFF de los investigados. Por eso, es indispensable el respeto a los principios de legalidad, subsidiariedad, especialidad y proporcionalidad de la medida, sobre todo, debiendo aplicarse solo ante situaciones que por necesidad y utilidad se requieran. Es importante la reflexión proporcionada a la ampliación del ámbito objetivo de actuación del agente encubierto informático, cuya regulación genera serias dudas en el respeto a la proporcionalidad de la medida y deja la puerta abierta a posibles violaciones de DDFF. La solución debe pasar por la observancia del juez caso por caso para que la autorización de su utilización se lleve a cabo, únicamente, en el respeto a estos principios y, por supuesto con la garantía del respeto a los DDFF de los investigados.

Quinta: El agente encubierto informático realiza la mayoría de su cometido en la fase de instrucción del proceso. El art. 282 bis LECrim apartado sexto otorga a este la posibilidad de actuar en canales cerrados, intercambiar archivos ilícitos con autorización específica y analizar los resultados de los algoritmos aplicados para identificar archivos ilícitos. Todo ello con el fin de recabar piezas probatorias suficientes que permitan romper la presunción de inocencia de los investigados. Por tanto, la función del agente encubierto informático es también esencial en la fase del juicio oral, donde su aportación como testigo, pero, igualmente, como perito informático, además de las pruebas documentales que entregue, aumenta su importancia en esta fase de enjuiciamiento con respecto al agente encubierto físico.

Sexta: Las redes sociales han experimentado un aumento fulgurante, principalmente gracias a adolescentes y menores desde una edad demasiado temprana. “Los delincuentes sexuales” han aprovechado esta coyuntura para llevar a cabo contactos con menores de edad para lograr obtener material pornográfico con el que alimentar sus filias. Esto nos hace defender la necesidad de una educación en la prevención tecnológica a menores de edad, así como la importancia del trabajo de los agentes en torno al patrullaje cibernético para paliar estos comportamientos cuando se produce el grooming, ya que, una vez facilitadas las imágenes pornográficas del menor, estas van a ser, en muchos casos, difundidas por foros de pedófilos, donde solo una actuación eficaz del agente encubierto informático puede conseguir la eliminación de esos archivos y el enjuiciamiento de los consumidores de esa pornografía.

Séptima: El marco de actuación del agente encubierto informático, una vez ha conseguido entrar en un canal cerrado de comunicación, cuya actividad se basa en el intercambio de material pornográfico de menores, es complicado. En la mayoría de esos casos, solo aquellos que compartan archivos podrán permanecer en el foro y se ganarán la confianza del resto de integrantes. En nuestro ordenamiento, no cabe la entrega controlada de este tipo de archivos, porque implicaría una nueva lesión de la indemnidad sexual de los menores protagonistas de los vídeos, aunque estos provengan de investigaciones ya cerradas. Por ello, para estos casos la solución más interesante consiste en acudir a actores y actrices mayores de edad con apariencia de menores, que den su consentimiento para que los videos que graben sean utilizados con el objetivo de que el agente pueda continuar la investigación.

Octava: En definitiva, la tecnología y las posibilidades de los delincuentes gracias a ella, no van a parar de desarrollarse. De tal forma que, va a ser imprescindible que el legislador esté atento a todos estos cambios para progresar normativamente. De lo contrario, la figura del agente encubierto informático y sus actuaciones quedarán inservibles en el momento que los delincuentes perfeccionen sus movimientos ante las medidas que, a día de hoy, puede materializar un agente encubierto informático. Es cierto, que el Derecho no se mueve tan rápido como lo hace la tecnología, entre otras cosas por la diferencia de financiación que reciben ambos ámbitos y las mayorías inalcanzables requeridas para promover una ley en el panorama político actual. Por ello, debemos aunar esfuerzos por mantener los más cerca posible al Derecho de la realidad vigente.

BIBLIOGRAFÍA

ABEL LLUCH, X., “La prueba pericial”, *Colección de formación continua Facultad de Derecho ESADE, Serie de estudios prácticos sobre los medios de prueba*, en GINÉS CASTELLET, N., (coord.), Bosch Editor, 2009.

BERNARDO SAN JOSÉ, A. “La restricción de los derechos fundamentales en las diligencias de investigación en el proceso penal y las exigencias derivadas del principio de proporcionalidad”, *Revista Ius*, Vol. 3, nº 24, 2009.

BUENO DE MATA, F., “El agente encubierto en Internet: Mentiras virtuales para alcanzar la justicia”, *Los retos del Poder Judicial ante la sociedad globalizada*, Universidade da Coruña, A Coruña, 2011.

BUENO DE MATA, F., “Fortalecimiento de Garantías procesales y medidas de investigación tecnológica”, *Ars Iuris Salmanticensis*, vol. 4, 2016.

BUENO DE MATA, F., *Las diligencias de investigación penal en la cuarta revolución industrial*, Thomson Reuters Aranzadi, Cizur Menor, 2019.

CAROU GARCÍA, S. “El agente encubierto como instrumento de lucha contra la pornografía infantil en internet. El guardián al otro lado del espejo”, *Cuadernos de la Guardia Civil: Revista de seguridad pública*, núm. 56, 2018.

CARRIZO GONZÁLEZ-CASTELL, A., “La infiltración policial en España como medio de investigación en la lucha contra la corrupción”. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 3, n. 2.

CLADERA ALBA, F., y GARCÍA MARTÍNEZ, G., “Blanqueo de capitales y agente encubierto en Internet” en BUENO DE MATA, F., (coord.), *Fodertics 5.0. Estudios sobre nuevas tecnologías y justicia*, Editorial Comares, 2016.

CRUZ DE PABLO, J. A. *Derecho Penal y nuevas tecnologías: aspectos sustantivos*, Difusión Jurídica, Barcelona, 2006.

CUERVO NIETO, C., “El delito de child grooming en el Derecho Penal español. Análisis del tipo penal y breves reflexiones”, disponible en <https://bit.ly/3n8fTp2>, (consulta 15-05-2022).

DÍAZ CORTÉS, L. M., “El denominado “child grooming” del artículo 183 bis del Código Penal: una aproximación a su estudio”, *Boletín del Ministerio de Justicia*, disponible en <https://bit.ly/3n7fuTT>, (consulta 14-05-2022).

DOLZ LAGO, M. J., “Child grooming y sexting: anglicismos, sexo y menores en el Código Penal tras la reforma del 2015”, *Diario la Ley*, disponible en <https://bit.ly/3Qxsks9>, (consulta 16-05-2022), Madrid, 2016.

FERNÁNDEZ TERUELO, J. G., “Cibercrimen. Los delitos cometidos a través de internet” *Constitutio Criminalis Carolina*, Oviedo, 2007.

GIMENO SENDRA, J. V., “El derecho de defensa”, *Constitución y proceso*, Tecnos, Madrid, 1988.

GIMENO SENDRA, V., (MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V.), *Derecho Procesal Penal*, Colex, Madrid, 1999.

GOMÉZ DE LIAÑO FONSECA-HERRERO, M., "Infiltración policial y proceso penal", *Investigación y prueba en el proceso penal*, N. González-Cuéllar Serrano y Á. Sanz Hermida (coords.), Madrid, 2006.

GONZÁLEZ ALONSO, F., DE CASTRO HERNÁNDEZ, R. M., *Mejorar la convivencia. Educación en valores y Derecho Educativo*, Tirant Humanidades, Valencia, 2019.

GONZÁLEZ-CUELLAR SERRANO, N., *Proporcionalidad y derechos fundamentales el proceso penal*, Colex, Madrid, 1990.

GUDÍN RODRÍGUEZ-MAGARIÑOS, F., “Algunas consideraciones sobre el nuevo delito de grooming”, *Delincuencia informática. Tiempos de cautela y amparo*, Thomson Reuters, Navarra, 2012.

LAFONT NICUESA, L., *El agente policial encubierto*, Tirant lo Blanch, Valencia, 2022.

MARTÍN IBÁÑEZ, E., “Dark web y Deep web como fuentes de ciberinteligencia utilizando minería de datos”, *Cuadernos de la Guardia Civil: Revista de seguridad pública*, nº 54, 2017.

MARTÍNEZ QUIROGA, J.F., “Entrada y registro, entregas vigiladas, apertura de paquetes y postales, agente encubierto y figuras afines”, curso de formación continua de fiscales *La investigación en el delito de tráfico de drogas y su incidencia en el juicio oral*, Centro de Estudios Jurídicos, 2015.

MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, McGraw-Hill, Madrid, 1996.

MOLINA MANSILLA, M. C., *Mecanismos de investigación policial: entrega vigilada y agente encubierto*, Barcelona, 2009.

MOLINA PÉREZ, T., “Técnicas especiales de investigación del delito. El agente provocador, el agente infiltrado y figuras afines”, “Anuario Jurídico y Escorialense, XLII, 2009.

ORTELLS RAMOS, M., “Exclusividad jurisdiccional para la restricción de derechos fundamentales y ámbitos vedados a la injerencia jurisdiccional”, *Medidas restrictivas de derechos fundamentales*, CGPJ, Madrid, 1996.

PANIZO GALENCE, V., “el ciber-acoso con intención sexual y el child-grooming”, *Quadernos de criminología: revista de criminología y ciencias forenses*, núm. 15, 2011.

PAZ RUBIO, J. M^a; MENDOZA MUÑOZ, J.; MORICHE, R. R; OLLÉ SESÉ, M., *La prueba en el proceso penal. Su práctica ante los Tribunales*, Madrid, 1999.

PERALS CALLEJA, J., “Técnicas de investigación del crimen organizado: el agente encubierto, confidente, regulación en España y validez de la prueba obtenida en el extranjero, problemas prácticos de la heterogénea regulación de la materia”, Cuadernos Digitales de Formación, 2010.

POZO PÉREZ, M. DEL, “El agente encubierto como medio de investigación de la delincuencia organizada en la ley de Enjuiciamiento Criminal Española”, *Criterio jurídico*, vol.6, Santiago de Cali, 2006.

POZO PÉREZ, M. DEL, “La entrega vigilada como medio de investigación de la delincuencia organizada en la Ley de Enjuiciamiento Criminal Española”, *Pensamiento jurídico*, núm. 28.

RAMOS VÁZQUEZ, J. A., “El llamado delito de “child grooming”: consideraciones acerca del nuevo artículo 183 bis del Código Penal”, disponible en <https://bit.ly/3bg4NM4>, (consulta 14-05-2022).

RIFÀ SOLER, J.M., “El agente encubierto o infiltrado en la nueva regulación de la LECrim.”, *Poder Judicial*, núm. 55.

RIZO GÓMEZ, M. B. “La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica” en *Justicia Penal y nuevas formas de delincuencia*, Tirant Lo Blanch, Valencia, 2017.

SAINZ-CANTERO CAPARRÓS, J. E., “Delitos contra la libertad e indemnidad sexuales (I)”, *Sistema de Derecho Penal. Parte Especial*, Dykinson, Madrid, 2016.

SÁNCHEZ ESCRIBANO, M. I., “Reflexiones sobre el child grooming. A propósito del libro *El delito de online child grooming o propuesta sexual telemática a menores*”, *Revista Jurídica de las Islas Baleares*, núm. 15, 2017.

SUITA PÉREZ, N., “La diligencia de investigación mediante la entrega vigilada”, *La actuación de la policía judicial en el proceso penal*, Madrid, 2006.

ZAFRA ESPINOSA DE LOS MONTEROS, M.R., *El policía infiltrado: los presupuestos jurídicos en el proceso penal español*, Tirant Lo Blanch, 2010.

ZARAGOZA TEJADA, J.I., “La modificación operada por la Ley 13/2015. El agente encubierto informático”, en FERNÁNDEZ BERMEJO, D. (coord.), y SANZ DELGADO E. (coord.), *Tratado de Delincuencia Cibernética*, Aranzadi, Navarra.

Legislación

1. Internacional

Convención de las Naciones Unidas contra la corrupción, art. 50, Mérida, 2003.

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos, art. 20, Palermo, 2000.

Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 19 de junio de 1990, al cual se adhirió el Reino de España mediante el Acuerdo de Adhesión de España el 25 de junio de 1991.

Convenio de asistencia judicial en materia penal entre Estados miembros de la Unión Europea (establecido mediante Acto del Consejo de 29 de mayo del 2000, DOCE C 197 de 12.07.2000).

Convenio del Consejo de Europa para la protección de lo niños contra la explotación y el abuso sexual, hecho en Lanzarote el 25 de octubre de 2007. Ratificado por España el 12 de marzo de 2009. *BOE* núm 274/2010, pp. 94858 a 94879.

Convenio del Consejo de Europa sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Ratificado por España el 23 de noviembre de 2001, *BOE* núm. 226/2010, pp. 78847 a 78896.

Decisión marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil. *DOUE* núm 13/2004, pp. 44 a 48.

Directiva 2011/93/UE del Parlamento y el Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, *DOUE* núm. 335/2011, pp. 1 a 14.

Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal (DOCE 1 de mayo de 2014).

Instrumento de Ratificación del Protocolo Facultativo de la Convención sobre los Derechos del Niño, relativo a la venta de niños, prostitución infantil y la utilización de niños en la pornografía, hecho en Nueva York el 25 de mayo del 2000. Ratificado por España el 5 de diciembre de 2001, *BOE* núm. 27/2002, pp. 3917 a 3921.

2. Nacional

Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 1/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, (BOE de 6 de octubre de 2015).

Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. (BOE 6 de diciembre de 2018).

Ley Orgánica 5/1999 de 13 de enero, de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves, (BOE de 14 de enero de 1999).

Real Decreto 769/1987, de 19 de junio, sobre regulación de la Policía Judicial, (BOE de 24 de junio de 1987).

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

Jurisprudencia

1. Sentencias del Tribunal Supremo

STS 104/2019, Sala II, Sección 1ª, 27 de febrero de 2019.

STS 1114/2002, Sala II, Sección 1ª, de 12 de junio de 2002.

STS 1124/1995, Sala II, Sección 1ª, 15 de diciembre de 1995.

STS 1140/2010, Sala II, Sección 1ª, de 29 de diciembre de 2010.

STS 140/2019, Sala II, Sección 1ª, de 13 de marzo de 2019.

STS 173/2018, Sala II, Sección 1ª, de 11 de abril de 2018.

STS 2331/2021, Sala II, Sección 1ª, de 10 de junio de 2021.

STS 679/1998, Sala II, Sección 1ª, de 28 de julio de 1998.

STS 690/2010, Sala II, Sección 1ª, de 1 de julio de 2010.

STS 750/2019, Sala II, Sección 1ª, de 13 de marzo de 2019.

STS 752/2010, Sala II, Sección 1ª, de 14 de julio de 2010.

STS 767/2007, Sala II, Sección 1ª, de 3 de octubre de 2007.

STS 97/2015, Sala II, Sección 1ª, de 24 de febrero de 2015.

2. Sentencias del Tribunal Constitucional

STC 229/1999, Sala Primera, de 13 de diciembre de 1999.

STC 25/2019, Sala Primera de 25 de febrero de 2019.

STC 253/2006, Sala Primera, de 11 de septiembre de 2006.

STC 50/1995, Sala Primera, de 23 de febrero de 1995.

3. Sentencia del Tribunal Europeo de Derechos Humanos

STEDH de 5 de febrero de 2008. Asunto Ramanauskas contra Lituania, Gran Sala, nº 18757/2006.

4. Sentencia de Tribunal Superior de Justicia

STSJCyL 14/2020, Sala de lo Civil y Penal, de 18 de marzo de 2020.

5. Sentencia de Audiencia Provincial

SAP de Navarra, Sección 2ª, nº 256/2016 de 14 de diciembre de 2016.