Facultad de Ciencias Sociales y Jurídicas de Elche

TRABAJO FIN DE GRADO

GRADO EN DERECHO

CURSO 2017/2018

POLICÍA JUDICIAL Y ACTOS DE INVESTIGACIÓN EN EL CAMPO DE LAS NUEVAS TECNOLOGÍAS

Iván Rabanaque Cerro

Tutora: Paloma Arrabal Platero

RESUMEN

En el presente TFG, se realizará un examen de los miembros de las Fuerzas y Cuerpos de Seguridad del Estado que llevarán a cabo labores de Policía Judicial, en concreto de los grupos especializados dedicados a combatir los delitos cometidos a través de las tecnologías de la información, que por la especial naturaleza de dicha tipología delictiva así se requiere y de los protocolos de actuación para su investigación. Así mismo, de algunos de los principales actos de investigación que han ido surgiendo y que llevan a cabo estos profesionales, tales como la infiltración y agente encubierto en Internet, tecnovigilancias, balizas y GPS, los virus espía o el uso de drones y su marco legal, con la reciente reforma de la Ley de Enjuiciamiento Criminal.

ÍNDICE

ABREVIATURAS

ART./ARTS.	Artículo/s
BIT	Brigada Central de Investigación Tecnológica
BCSI	Brigada Central de Seguridad Informática
CE	Constitución Española
DDAT	Departamento de Delitos en Altas Tecnologías
EDITE	Equipos De Investigación Tecnológica
FCS	Fuerzas y Cuerpos de Seguridad
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
FGE	Fiscalía General del Estado
GDT	Grupo de Delitos Telemáticos
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Suscriber Identity
IP	Internet Protocol
LECRIM	Ley de Enjuiciamiento Criminal
LO	Ley Orgánica
LOFCS	LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad
LOPJ	Ley Orgánica del Poder Judicial
RD	Real Decreto
STC	Sentencia del Tribunal Constitucional
TC	Tribunal Constitucional
STS/SsTS	Sentencia/s del Tribunal Supremo
TIC	Tecnologías de la Información
UCO	Unidad Central Operativa
UDEF	Unidad de Delincuencia Económica y Fiscal

UIT	Unidad de Investigación Tecnológica
VANT	Vehículo Aéreo no Tripulado

INTRODUCCIÓN

El presente trabajo pretende examinar algunos de los principales actos de investigación que se están llevando a cabo para combatir los delitos surgidos con la aparición de las nuevas tecnologías, con especial análisis a las Fuerzas y Cuerpos de Seguridad del Estado que tienen encomendada la persecución de esta especial tipología delictiva, analizando qué especialización cuentan para poder llevar a buen término su labor, así como los protocolos de actuación que siguen para su investigación.

Este TFG se divide en dos bloques diferenciados, el primero de los cuales está dedicado a la Policía Judicial, en concreto de las Fuerzas y Cuerpos de Seguridad del Estado y los grupos especializados que la integran, sus protocolos de actuación y las principales tipologías delictivas que persiguen. El segundo bloque estará dedicado a los principales actos de investigación en el campo de las nuevas tecnologías.

Para averiguar si se ha producido o no un hecho delictivo, circunstancias en las que se ha producido y su presunto autor, hay que efectuar una serie de actividades, conocidas como actos de investigación y que lleva cabo la Policía Judicial, motivo por el que también se les conoce como diligencias policiales. En este sentido, habrá que tener en cuenta como han afectado las nuevas tecnologías a la comisión de hechos delictivos, ya que el desarrollo tecnológico e implantación masiva que se ha ido produciendo en informática y comunicación, permite hablar de un entorno digital, ya que dicha tecnología se usa para múltiples aspectos de la vida cotidiana, comunicar, jugar, estudiar, trabajar, pero no siempre se hace un buen uso de Internet, siendo un terreno abonado para que los delincuentes lo aprovechen. Y esto es así por las especiales características que favorecen a los delincuentes para cometer sus ciberataques, tales como los pocos recursos económicos necesarios para llevarlos a cabo, la capacidad de realizarlos desde y hasta cualquier lugar y las posibilidades de anonimato de su autor, no facilitan la identificación de sus responsables.

Como no podía ser de otra manera, las Fuerzas y Cuerpos de Seguridad del Estado se servirán también de estas nuevas tecnologías para la investigación de los delitos, ya que los avances tecnológicos constituyen una potente herramienta de trabajo a través de diligencias como la tecnovigilancia, el agente encubierto en Internet, los drones, los sistemas de captación de imágenes térmicas o de visión nocturna, reconocimiento

biométrico de personas o el uso de la tecnología GPS, todo bajo el paraguas de la última reforma de la LECrim por la LO 13/2015, de 5 de octubre, que supuso un importante impulso en la lucha contra la delincuencia en el ciberespacio. Ello, no obstante, la utilización de estos actos de investigación puede vulnerar los derechos fundamentales de los investigados, y por tanto, su práctica deberá realizarse –en la mayoría de ocasiones- con autorización judicial.

En la investigación de estos delitos los investigadores deberán actuar con rapidez, ya que los vestigios desaparecen en un corto espacio de tiempo y se hace difícil averiguar quién ha sido el autor del delito. Autores, que suelen ser profesionales cualificados que buscan un beneficio personal y en el seno de una organización criminal, con una rápida reinvención, obligando a quienes los investigadores a estar al día en este campo.

Un trabajo espero que interesante y actual, ya que los delitos cometidos a través de las TIC no dejan de crecer y cualquier persona física o jurídica está expuesto a ellos.

EPIGRAFE 1. LA POLICÍA JUDICIAL

1.1. INTRODUCCIÓN

Las Fuerzas y Cuerpos de Seguridad del Estado tienen como misión la protección del libre ejercicio de los derechos y libertades de los ciudadanos y de garantizar la seguridad ciudadana[1]. Dentro de estos institutos armados, se encuentra la Policía Judicial, cuya organización se llevará a cabo con miembros de los dos Cuerpos de Seguridad del Estado, que habrán de recibir una formación especializada, configurándose la Policía Judicial, como una especialidad policial, y cuenta entre sus deberes auxiliar al Poder Judicial mediante el desempeño de sus funciones y facilitar, con la elaboración de los correspondientes atestados, el proceso penal.

Esta participación en el proceso judicial será la finalidad de estas unidades policiales, ya que como consecuencia de la investigación, averiguación del delito y de los delincuentes, tendrán que elaborar informes técnicos y atestados de los hechos antijurídicos investigados. Las partes utilizarán las diligencias realizadas en el seno del proceso[2].

1.2. MARCO LEGAL

Las Fuerzas y Cuerpos de Seguridad (en adelante, FCS), son institutos armados que de acuerdo al art 104 de la Constitución Española (en adelante, CE), "tendrán como misión de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana" y remite a su desarrollo legislativo, que será la LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad (en adelante, LOFCS).

La LOFCS especifica quienes son miembros de las FCS, que son: 1.- Las Fuerzas y Cuerpos de Seguridad del Estado (en adelante, FCSE), dependientes del Gobierno de la Nación, compuestos por la Policía Nacional y la Guardia Civil, 2.- los Cuerpos de Policía dependientes de las Comunidades Autónomas cuyas competencias han sido delegadas y asumidas[3], el Cuerpo de Policía de la Ertzaintza en el País Vasco,

[1] Art. 11.1 de la LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.
[2] NÚÑEZ IZQUIERDO, F. "La policía judicial. El auxilio con la administración de justicia en la investigación criminal". http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4759-la-policia-judicial-el-auxilio-con-la-administracion-de-justicia-en-la-investigacion-criminal/ Marzo 2002.Consultado el 13 de abril de 2018.
[3] Hay comunidades que no han creado cuerpos de policía autonómicos, pese a que su estatuto lo prevea. Este es el caso de la Comunidad Valenciana, que en el art. 55 ya dispone su creación. Actualmente aún

el Cuerpo de la Policía Foral de Navarra y el Cuerpo de Policía de los Mossos d´Esquadra en Cataluña y por último Los Cuerpos de Policía dependientes de las Corporaciones Locales en aquellos municipios donde se hayan creado dichos Cuerpos[4].

El art 126 CE establece que la Policía Judicial depende de los Jueces, de los Tribunales y del Ministerio Fiscal en sus funciones de averiguación del delito y descubrimiento y aseguramiento del delincuente, en los términos que la ley establezca.

No se ha desarrollado una legislación integral sobre Policía Judicial. Su regulación se encuentra dispersa en diversos artículos de la Ley de Enjuiciamiento Criminal (en adelante, LECrim) y en otras disposiciones de variado objeto y rango normativo, principalmente en la LO 6/1985, de 1 de julio, del Poder Judicial (en adelante, LOPJ) -modificada a estos efectos por LO 19/2003, de 23 de diciembre-, cuyo Título III de su Libro VII -arts 547 a 550- se dedica a la regulación de la Policía Judicial; en la ya mencionada LOFCS, que, en el capítulo V de su Título II, configura las denominadas "Unidades de Policía Judicial", así como en el RD 769/1987, de 19 de junio, sobre regulación de Policía Judicial, modificado por RD 54/2002, de 18 de febrero, para incorporar a las Comisiones de Coordinación de Policía Judicial, a aquellas Comunidades Autónomas con competencia estatutaria en esta materia.

El resultado de la evolución legislativa a partir de la estructuración jurídico-política establecida por la CE, ha determinado la configuración de un sistema de Policía Judicial que se caracteriza por su complejidad, en el que coexisten dos modelos: 1º de Policía Judicial Genérica, con la obligación general de auxiliar a la Justicia que compete a todos –art 118 CE-, encuentra su origen en el art 283 LECrim, dando lugar a una Policía Judicial de carácter colaborador, al cual se refiere la LOPJ, que indica en su exposición de motivos que la Policía Judicial (…) "es una (…) institución que coopera y auxilia a la Administración de Justicia". Así, el art 547 LOPJ establece que la función de la Policía Judicial comprende el auxilio a los juzgados y tribunales y al Ministerio

continúa con la Unidad adscrita de la Policía Nacional para el cumplimiento de alguna de las funciones de lo que sería el cuerpo autonómico.

[4] El Cuerpo de la Policía Local no existe en todos los municipios de España. En principio, la decisión de crearlo corresponde a los Ayuntamientos que, por razones organizativas y funcionales, así lo estimen conveniente. Algunas leyes autonómicas se refieren a este aspecto, como el art. 34 de la ley 17/2017, de 13 de diciembre, de la Generalitat, de coordinación de policías locales de la Comunitat Valenciana que establece "1. Los municipios de la Comunitat Valenciana con población superior a 5.000 habitantes tendrán la obligación de crear un cuerpo de policía local y 2. Los municipios de la Comunitat Valenciana con población inferior a 5.000 habitantes podrán crear sus propios cuerpos de policía local si lo estiman oportuno, en función de sus necesidades, de acuerdo con lo dispuesto en la normativa estatal de referencia y en esta ley".

Fiscal en la averiguación de los delitos y en el descubrimiento y aseguramiento de los delincuentes. 2º de una Policía Judicial Específica: un modelo policial concentrado o en sentido estricto, a la que se refieren los 548 y siguientes de la LOPJ y 29 y siguientes LOFCS. Este modelo responde a un concepto de Policía Judicial que se basa en los principios de unidad de dirección y especialización, por ello el RD 769/1987, centra su regulación alrededor de lo que el art 30.1 LOFCS, denomina Unidades Orgánicas de Policía Judicial, integradas por funcionarios del Cuerpo de Policía Nacional y por miembros de la Guardia Civil[5] y cuyos principios rectores son los de permanencia, estabilidad y especialización, con estricta sujeción o dependencia funcional respeto de Jueces, Tribunales y Ministerio Fiscal en la ejecución de cometidos relativos a la averiguación del delito y descubrimiento y aseguramiento del delincuente.

Si bien la LOFCS establece que las Policías Autonómicas y Locales se constituyen en colaboradores o partícipes[6] de la función de Policía Judicial, cuyo ejercicio se atribuye a las Fuerzas y Cuerpos de Seguridad del Estado -art 11.1.g) LOFCS- que ejercitan su competencia mediante unidades constituidas sobre criterios de especialidad y exclusividad -art 30.1 LOFCS-, nada se opone a su coexistencia con la indicada legalidad autonómica, ello no obstante en la actualidad la Ertzaintza, los Mossos d´Escuadra y la Policía Foral de Navarra cuentan con Unidades Orgánicas de Policía Judicial[7], que coexisten con las de las FCSE.

Así, el art 282 de la LECrim, establece que "La Policía Judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la Autoridad Judicial", y en el mismo sentido se pronuncia el art 29 de la LOFCS, que establece "1. Las funciones de Policía Judicial que se mencionan en el artículo 126 de la Constitución serán ejercidas por las Fuerzas y Cuerpos de Seguridad del Estado, a través de las unidades que se regulan en el presente Capítulo. 2. Para el cumplimiento de dicha función tendrán carácter colaborador de las

[5] Art 7 RD 769/1987, de 19 de junio
[6] Arts 29.2, 38.2.b, 46 y 53.1.e) LOFCS.
[7] INSTRUCCIÓN Nº 1/2008 de la FGE, *sobre la dirección por el Ministerio Fiscal de las actuaciones de la Policía Judicial*. p.6.

Fuerzas y Cuerpos de Seguridad del Estado el personal de Policía de las Comunidades Autónomas y de las Corporaciones Locales."

Dentro del espacio europeo, se recogen las normas de cooperación policial del sistema judicial europeo[8] y se crean dos organismos mundialmente conocidos, EUROPOL Y EUROJUST, cuya finalidad es la lucha contra el terrorismo, trata de seres humanos, delitos contra los niños, tráfico de drogas y armas, el crimen sea o no organizado, la corrupción y el fraude, cuando afecten a países miembros de la Unión Europea y en colaboración con otras Organizaciones y Estados para, tal y como dice el tratado, conseguir un alto grado de seguridad ciudadana entre la población de los Estados miembros, luchando contra cualquier acto grave de delincuencia mediante la cooperación policial y judicial en materia penal.

1.3. FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO ESPECIALIZADOS EN LA INVESTIGACIÓN TECNOLÓGICA

Para la investigación de los delitos informáticos y de los delitos que pese a no ser informáticos se han cometido a través de las nuevas tecnologías, se requiere que los cuerpos policiales que investigan estén especializados, y en este sentido se ha creado dentro de la Policía Nacional y de la Guardia Civil grupos especializados en la investigación de estos delitos.

Al margen de que algunos cuerpos de policía autonómicos pudieran contar con grupos especializados en esta materia, se va a centrar el estudio en las unidades pertenecientes a las FCSE.

1.3.1. POLICÍA NACIONAL: UNIDAD DE INVESTIGACIÓN TECNOLÓGICA (UIT)

La continua evolución de Internet y el crecimiento exponencial de los delitos a través de las nuevas tecnologías de la información (en adelante, TIC), hicieron que con la modificación de la Dirección General de la Policía del año 2013, pasara de ser una Brigada (Brigada de Investigación Tecnológica) dentro de la Unidad de Delincuencia

[8] Título VI, arts. 29 al 42 del Tratado de Maastricht de 1992.

Económica y Fiscal –UDEF– a una Unidad Central independiente y compuesta por dos brigadas ante el aumento de las prácticas ilícitas a través de Internet.

La Unidad de Investigación Tecnológica (en adelante, UIT) asume la investigación y persecución de las actividades delictivas que impliquen la utilización de las TIC y el ciberdelito de ámbito nacional y transnacional, relacionadas con el patrimonio, el consumo, la protección al menor, la pornografía infantil, delitos contra la libertad sexual, contra el honor y la intimidad, redes sociales, fraudes, propiedad intelectual e industrial y seguridad lógica. Esta unidad asume las competencias de coordinación a nivel nacional e internacional, y de formación de los miembros del resto del Cuerpo de Policía Nacional y otros cuerpos policiales en este ámbito. Además actuará como Centro de Prevención y Respuesta E-Crime del Cuerpo de Policía Nacional[9].

Tienen encomendada como misión obtener las pruebas, perseguir a los delincuentes y ponerlos a disposición judicial, contando con herramientas como la formación continua de los investigadores, la colaboración de instituciones públicas y privadas, la participación activa en los foros internacionales de cooperación policial y la colaboración ciudadana.

La UIT está compuesta aproximadamente por un equipo de 85 funcionarios de diferentes escalas y perfiles, a fecha de 2016, que combinan la capacitación técnica con la experiencia policial. Cuenta con ingenieros, peritos y técnicos informáticos que, además de reunir las capacidades tecnológicas que requiere su trabajo, participan en todo tipo de foros nacionales e internacionales. En el año 2015, la UIT realizó 516 investigaciones entre las que destacan 188 relacionadas con la explotación sexual infantil online, 76 fraudes digitales (especialmente en las telecomunicaciones), 67 de seguridad lógica (antipiratería, ciberataques o hacktivismo) y 66 en redes sociales. Además, la Sección Técnica participó en 119 operaciones para realizar volcados en caliente o gestionar evidencias digitales procedentes de ordenadores y otros dispositivos[10].

La UIT cuenta con una Sección Técnica, que está bajo la dependencia del Comisario Principal de la UIT, que alberga el mayor conocimiento técnico de toda la

[9] POLICÍA JUDICIAL.UIT. https://www.policia.es/org_central/judicial/estructura/funciones.html
[10] Revista Red Seguridad nº 072, Primer trimestre 2016, Bormart S.A. pp. 8-9. Disponible en: http://www.redseguridad.com/revistas/red/072/index.html#8

UIT y se encarga de dar soporte tanto a las Brigadas de la UIT como a todas las unidades de Policía, con cuestiones como el análisis de los equipos durante las operaciones, formación del personal del Cuerpo de Policía Nacional y otros Cuerpos de Policía nacionales y extranjeros, participación en foros de ámbito internacional (Interpol, Europol, Consejo de Europa,...) análisis forenses de los equipos o I+D respecto a las herramientas y técnicas de investigación tecnológica, donde cuentan con un laboratorio con potentes herramientas y equipos de los que extraer información.

De esta Unidad dependerán la Brigada Central de Investigación Tecnológica (en adelante, BIT) y la Brigada Central de Seguridad Informática (en adelante, BCSI).

1.3.1.1. Brigada Central de Investigación Tecnológica (BIT)

La BIT es la unidad policial destinada a responder a los retos que plantean las nuevas formas de delincuencia. Le corresponden la investigación de las actividades delictivas relacionadas con la protección de los menores, la intimidad, la propiedad intelectual e industrial y los fraudes en las telecomunicaciones.

Entre sus actuaciones se encuentran las amenazas, injurias, calumnias, ya sean realizadas por correo electrónico, sms, tablones de anuncios, foros, newsgroups, web...; la pornografía infantil y la protección al menor en el uso de las nuevas tecnologías, así como los fraudes en el uso de las comunicaciones, como puede ser la piratería de señales de televisión privada.

Hasta el año 2013, esta Brigada asumía dentro de la Policía Nacional los delitos en la Red. En la actualidad se ha centrado en los delitos relacionados con el abuso infantil online y en las redes sociales, y los delitos contra las personas más que en los de patrimonio.

La BIT se divide en dos secciones: La Sección de Protección al Menor y La Sección de Redes.

La Sección de Protección al Menor, a su vez está dividida en tres grupos: 1.- el de colaboración con el FBI, mediante el cual se organizan y coordinan operaciones en colaboración con la institución policial federal estadounidense; 2.- el de investigación

de la "red oculta" o de Redes *Peer to Peer (P2P)*[11] y 3.- de Protección al Menor, que con investigaciones dirigidas a la localización del centro de producción de la pornografía infantil, desde donde se vende, distribuye, exhibe o facilita utilizando prácticamente todas las aplicaciones de Internet y a la coordinación de la oficina virtual con la Interpol para la identificación de víctimas. Las principales dificultades con las que se encuentran son el anonimato en la Red, al hacer uso de herramientas opacas para ocultarse[12].

La Sección de Redes se creó a principios de 2014, con la expansión en el uso de las redes sociales. La actividad de la sección se divide en la monitorización para ver qué está pasando en Internet de forma general, detectar "modus operandi" nuevos y por otro en las redes sociales, especialmente con temas *trending topic*[13], llevando a cabo la elaboración de informes de control y prevención, sobre actividades que sin ser delictivas puedan resultar nocivas o altamente peligrosas especialmente para los menores. También asumen la investigación de otros delitos como el juego online, la extorsión, injurias o calumnias. Entre los contenidos investigados están los que hacen referencia a la violencia específica al racismo y la xenofobia, agresiones brutales y ataques a la integridad moral de personas, en espacial disminuidos y menores de edad. Contenidos que contravienen normas de circulación vial, como las carreras ilegales en circuitos urbanos, los que hacen referencia a la Anorexia y Bulimia[14] y otros contenidos en general como los suicidios colectivos, maltratos a animales o técnicas para sustracción en grandes almacenes[15].

1.3.1.2. Brigada Central de Seguridad Informática (BCSI)

La BCSI es la unidad policial también destinada a responder a los retos que plantean las nuevas formas de delincuencia, respecto investigación de las actividades delictivas que afecten a la seguridad lógica y a los fraudes.

---

[11] Redes Punto a Punto. Es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.
[12] Revista Red Seguridad ... op. cit. p. 10.
[13] Tema de tendencia o tema del momento. Para más información véase el blog: http://www.avanteservices.com/es/blog/?p=350
[14] Noticia relacionada: https://www.eldiario.es/hojaderouter/internet/paginas-ana-mia-anorexia-bulimia-leyes-espana_0_298170489.html
[15] Revista Red Seguridad 072…", op. cit. p. 11.

Entre sus actuaciones se encuentran los fraudes en Internet, que abarcan estafas, uso fraudulento de tarjetas de crédito, fraudes en subastas, comercio electrónico, bancas virtuales, cartas nigerianas, solicitud engañosa de transferencia, pirámides financieras, ofertas de trabajo, casinos y apuestas. Por otro lado la seguridad lógica, como son virus, ataques de denegación de servicio, sustracción de datos, hacking, descubrimiento y revelación de secreto, suplantación de personalidad y sustracción de cuentas de correo electrónico. Y por último la piratería de programas de ordenador, de música y de productos cinematográficos, la falsificación de soportes informáticos, fonogramas, videogramas, producción, distribución y venta de software profesional y lúdico. También el «cracking» para la eliminación de protección de los programas originales.

La BCSI está dividida en dos secciones, la sección de "Seguridad Lógica" y la sección de "Fraudes digitales".

La sección de "Seguridad Lógica" está especializada en la persecución de la piratería online, los ciberataques y el *hacktivismo*, y todas aquellas acciones que supongan la vulneración de las medidas de seguridad de los sistemas informáticos. Para esta tarea cuenta con dos grupos, el de antipiratería y el de ciberataques. El primero de ellos se encarga de averiguar los delitos contra la propiedad intelectual, como pueden ser la descarga de películas, series, videojuegos o música[16]. Este grupo investiga el intercambio de archivos, a requerimiento judicial o del Ministerio fiscal. Dentro de este procedimiento, las investigaciones que se han llevado en la Brigada, estaban dirigidas contra los responsables de páginas web que facilitaban las descargas de copias ilícitas a cambio de importantes beneficios económicos basados principalmente en la publicidad insertadas en dichos portales[17].

El grupo dedicado a los ciberataques es el que quizás más complejidad tiene a la hora de llevar cabo la investigación, por cuestiones como la anonimación, la complejidad judicial internacional, las redes *P2P*, el *crime as a service*[18], los *blackmarkets*, el cifrado de las comunicaciones y los equipos, entre otros. Son numerosos los obstáculos para la descubrir a los presuntos delincuentes, dado que para

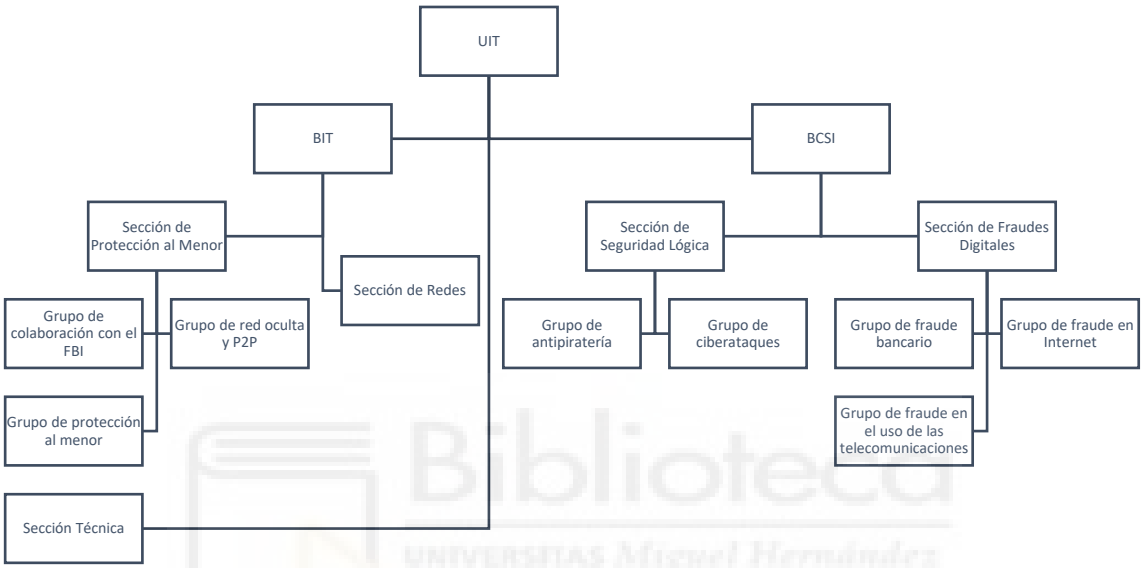
[16] El 95 % de la piratería se produce a través de Internet. Revista Red Seguridad 072…", op. cit. p. 9.

[17] Noticias relacionadas: https://www.20minutos.es/noticia/1471881/0/detenidos/youkioske/pirateria/http://www.europapress.es/sociedad/noticia-policia-cierra-webs-descarga-ilegal-peliculas-pepito-series-pepito-detiene-administradores-20141203151714.html Consultado el 20 de abril de 2018

[18] Crimen como servicio, ciberdelincuencia al alcance de cualquiera. Para más información véase: https://aunclicdelastic.blogthinkbig.com/crime-as-a-service-la-ciberdelincuencia-al-alcance-de-cualquiera/ Consultado el 20 de abril de 2018

acceder a un servidor situado en otro país debe solicitarse a través de una comisión rogatoria, que es un procedimiento más lento de lo que requeriría, y para entonces los ciberdelincuentes ya pueden haber cambiado los parámetros o su situación[19].

La Sección de Fraudes Digitales está compuesta por tres grupos: El grupo de fraude bancario, el grupo de fraude en Internet y el de fraude en el uso de las telecomunicaciones.



Organigrama de la UIT. Elaboración propia.

1.3.2. GUARDIA CIVIL: GRUPO DE DELITOS TELEMÁTICOS (GDT)

La Guardia Civil, en el ámbito de la investigación criminal, también es responsable de la investigación de los denominados delitos informáticos o Cibercrimen. De la misma manera, en el ámbito de las TIC, existen amenazas a la Ciberseguridad, suponiendo un nuevo campo en el que la Guardia Civil debe llevar cabo no solo sus funciones de Policía Judicial (investigación de delitos), sino las de Seguridad Ciudadana en este nuevo ámbito de actuación que es el Ciberespacio.

Habida cuenta de que desde su aparición el fenómeno del Cibercrimen ha evolucionado de forma exponencial, la Guardia Civil, al igual que otras muchas Instituciones, ha tratado de dar una respuesta global, racional, y eficaz a dicho

[19] Revista Red Seguridad 072…", op. cit. p. 9.

fenómeno. Actualmente, se pueden encontrar varias Unidades de la Guardia Civil implicadas en la lucha contra el fenómeno "Ciber", ya sea en su vertiente del Cibercrimen, el Ciberterrorismo, o la Ciberseguridad. Además de las Unidades "especializadas", se debe tener en cuenta que prácticamente en todas las Unidades de Policía Judicial, existen grupos dedicados a actividades en el entorno "Ciber"[20].

La Guardia Civil creó el Grupo de Delitos Informáticos en el año 1996, dentro de la Unidad Central Operativa (en adelante, UCO), para atender a las pocas denuncias que había entonces por los llamados delitos informáticos. En 1998 cambió su denominación por la de Departamento de Delitos en Altas Tecnologías (DDAT) asumen las competencias sobre los recién aparecidos fraudes en el sector de las telecomunicaciones[21].

Con la socialización de Internet y el crecimiento de los hechos delictivos, se amplía el abanico de competencias de investigación, que alcanza a todas aquellas conductas delictivas realizadas a través de los sistemas de información o contra éstos, lo que se conoce popularmente como el cibercrimen. En el año 2000 pasó a denominarse Departamento de Delitos Telemáticos y en el 2003, con una restructuración de la UCO, adquirió el actual nombre de Grupo de Delitos Telemáticos (en adelante, GDT). Estos cambios se acompañaron de la creación de los Equipos de Investigación Tecnológica (en adelante, EDITE) en cada una de las provincias de España, equipos descentralizados y dependientes. El esfuerzo principal del GDT y de los EDITE ha sido, desde su creación, la investigación de la delincuencia que se vale de las redes y sistemas de información para su comisión[22].

También asumen funciones para fomentar un uso seguro de las nuevas tecnologías, consciente de que a la larga este esfuerzo ayudará a minimizar el impacto de la delincuencia[23].

---

[20] LORENZANA GONZÁLEZ, C. "Ponencia: La Investigación de delitos telemáticos por la Guardia Civil, y sus capacidades al servicio del Ministerio Fiscal". p.4. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20escrita%20Sr%20Lorenzana.pdf?idFile=e14972b0-5d5a-40d6-8940-f1ef8152c3f9

[21] La Unidad, consultado el 13 de abril de 2018, disponible en el link: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

[22] La Unidad, consultado el 13 de abril de 2018, disponible en el link: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

[23] La Unidad, consultado el 13 de abril de 2018, disponible en el link: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

Sus cometidos se centran en investigaciones sobre los llamados delitos informáticos y los fraudes en el sector de las telecomunicaciones, y en apoyar a los restantes Grupos y Departamentos de la UCO en la que se encuadra.

Ello no obstante, por la peculiaridad del medio tecnológico en que trabaja, su personal precisa de una formación continuada, que influye directamente sobre la eficacia de sus actuaciones.

En este sentido, dentro del trabajo del GDT, su presencia continuada en seminarios y conferencias internacionales, lo que le ha permitido crear con una red de contactos policiales a nivel internacional, esencial en la resolución de determinadas investigaciones. El GDT actualmente es miembro y participa activamente en los grupos de trabajo de Interpol de Europa y Latinoamérica, en el Foro Internacional del G-8 para el cibercrimen, y en el grupo de Europol[24].

El GDT está dividida en distintas secciones, como son la Sección de Investigación, que a su vez se divide en diferentes equipos (equipo de Pedofilia, Fraudes, Hacking y Propiedad Intelectual). La Sección de Análisis (equipo de Análisis y de I+D y por último la Sección de Delitos Tecnológicos, cuyas misiones se centran en la elaboración de inteligencia prospectiva, la coordinación (tanto a nivel nacional como internacional), y la creación y difusión de procedimientos y protocolos para unificar las actuaciones de la Guardia Civil en este ámbito.

De entre las misiones del GDT, caben destacar el desarrollo de investigaciones relacionadas con la delincuencia informática, apoyo a aspectos técnicos del resto de investigaciones de la UCO, formación del personal de los equipos de investigación tecnológica de las distintas Comandancias o representar y promover la participación de la Guardia Civil en determinados foros y encuentros internacionales sobre cibercrimen (EWPITC, G-8, GTLDTI, FIEC, EUROPOL)[25].

Resulta importante destacar que muchas de estas funciones no son exclusivas del GDT, sino que existen otras Unidades en el seno de la Guardia Civil que también llevan a cabo actividades como el apoyo técnico, realizados por el Servicio de Criminalística y

[24] La Unidad, consultado el 13 de abril de 2018, disponible en el link: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

[25] LORENZANA GONZÁLEZ, C. "Ponencia: La Investigación de…" op. cit. p.p. 5-6.

la Unidad Técnica de Policía Judicial cuando éstos atañen a otras Unidades diferentes a la UCO[26].

1.4. PROTOCOLOS DE ACTUACIÓN

En referencia a los protocolos de actuación, cabe mencionar la Estrategia de Ciberseguridad Nacional, que es el marco de referencia de un modelo que coordina los distintos actores en seguridad. Esta Estrategia crea una estructura orgánica que se integra en el marco del Sistema de Seguridad Nacional, para la prevención, defensa, detección y respuesta a los ciberataques[27].

Para la investigación de los delitos de las TIC, se diferencian tres fases, una primera fase previa, la de investigación y la incriminatoria[28].

En una primera fase previa, se comprueba la existencia o no del delito. La misma se iniciará a partir del concomimiento de la comisión delictiva. Desde las distintas páginas webs de los grupos UIT o del GDI facilitan este tipo de comunicaciones, ofreciendo distintas posibilidades en las que el usuario puede colaborar o informar sobre una actividad que pudiera ser delictiva o directamente realizar una denuncia electrónica[29].

En esta fase suele ser cuando se comprueba la información, mediante diligencias como la inspección ocular donde haya podido pasar la comunicación delictiva, pudiéndose adoptar medidas sobre los medios utilizados para su comisión como aislar el equipo utilizado (pcs, smartphone,…) buscando los indicios suficientes para la comprobación de la información, de la perpetración del delito y que permita incoar la investigación.

Es necesario señalar que aislar un equipo informático podría vulnerar el derecho fundamental a la intimidad de su propietario, por el simple hecho de que al realizar un examen del equipo se examina en su totalidad, donde en la mayoría de los casos contendrá información personal y privada, y donde el mejor exponente de la ponderación realizada por nuestro Tribunal Constitucional (en adelante, TC) entre la

[26] LORENZANA GONZÁLEZ, C. "Ponencia: La Investigación de…" op. cit. p.p. 5-6.
[27] La Estrategia de Ciberseguridad Nacional, 2013, Disponible en: http://www.dsn.gob.es/es/file/146/download?token=Kl839vHG Consultada el 15 de abril de 2018
[28] De acuerdo con la INSTRUCCIÓN Nº 1/2008 de la FGE… op. cit. p.p. 18-22.
[29] Policía Nacional: https://denuncias.policia.es/OVD/; Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/pinformar.php

protección de los derechos fundamentales de la persona y el empleo de la tecnología, cuando se persigue un fin legítimo como es la investigación criminal por parte de las autoridades judiciales y policiales, lo representa la STC 173/2011, de 7 de noviembre, en donde expresamente se pronuncia sobre la necesidad de establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas -en particular, la intimidad personal- a causa del uso indebido de la información así como de las TIC durante la investigación criminal.

Nuestro TC dispone así, que cualquier injerencia en el contenido de un ordenador personal deberá venir legitimada, en principio, por el consentimiento de su titular, o bien por una previa resolución judicial, salvo en los casos en los que se estime necesaria y urgente la actuación policial, porque exista un riesgo concreto e inminente para la vida de las personas como consecuencia de la utilización de tales dispositivos[30].

Durante la segunda fase la Policía Judicial tendrá la labor de poder identificar las conexiones que tengan relación con el delito investigado y recabar los datos de tráfico para poder situar donde se encuentran los equipos, identificar a los abonados de la conexión utilizada, para una vez hecho esto, conseguir el fin último que no es otro que la identificación del usuario del equipo.

Como ya se ha mencionado, para la investigación de los delitos de las TIC, se requieren conocimientos y formación específica de Internet y el funcionamiento de la red de redes. Cuando se realiza una conexión del equipo con el proveedor de acceso a Internet, este asigna lo que se conoce como número de dirección IP[31], que se integra por las claves de acceso que los proveedores de servicios de Internet asignan a cada ordenador o terminal en el momento en que se conecta a Internet, el cual permite identificar de forma indubitada a través de dichos proveedores el número telefónico desde el que se produce la conexión. Dentro de este proceso de comunicación se producen lo que se conoce como *datos sobre el tráfico*. El Convenio de Budapest entiende que por *datos sobre el tráfico* se entenderánlos datos informáticos relativos a

[30] ORTIZ PRADILLO J.C., *La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, ed. Fundación Alternativas, disponible en: http://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf Madrid, 2013, p.p. 23-24.

[31] IP es un número único que identifica cada dispositivo que se conecta a la red. Los PCs, los móviles, los televisores e incluso las páginas web tienen una dirección de Internet Protocol asignada, y jamás habrá dos números iguales, sirve para identificar a las personas que se conectan a Internet. Para más información ver: https://computerhoy.com/noticias/internet/como-geolocalizar-direccion-ip-72691 Consultado el 24 de mayo de 2018.

una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente. Gracias a estos datos, es posible conocer identificar el equipo, ubicación y abonado de la conexión.

El art. 588 ter k de la LECrim, regula la identificación de los equipos y usuarios mediante la obtención del número IP. Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en Internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión de algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.

Con anterioridad a la aprobación de este precepto, la Circular n.º 1/2013 de la Fiscalía General del Estado (FGE), en esta materia ya establecía que los rastreos policiales para localizar direcciones IP pueden realizarse sin necesidad de autorización judicial, ya que no se trata de datos confidenciales preservados al conocimiento público. Tras la averiguación de dicha IP, las subsiguientes actuaciones de identificación y localización de quien sea la persona que tiene asignado dicha IP se deben llevar a cabo bajo control de la Autoridad Judicial.

El Art. 588 ter l de la LECrim, sobre la identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes determina que “1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado

o la tarjeta utilizada para acceder a la red de telecomunicaciones" y "2. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 ter d

La solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior".

El tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo establecido en el artículo 588 bis c.

El IMSI, que son las siglas de International Mobile Suscriber Identity, se refiere a la identidad internacional del abonado a un móvil, es un código de identificación único para cada dispositivo móvil integrado en la tarjeta SIM.

El IMEI son las siglas de International Mobile Station Equipment Identity, y se refiere a la identidad internacional del equipamiento móvil. Se trata del número de serie que identifica el terminal físicamente, no se utiliza para establecer la conexión, solo se comprueba por razones de seguridad antes de iniciar la comunicación.

La captación de tales números por las FCSE, a efectos de investigación penal, es posible mediante el empleo de medios técnicos o no técnicos. Una de las formas empleadas mediante medios técnicos, es la utilización de un escaneado o barrido realizado a través de instrumentos electrónicos y para que puedan ser detectados han de ser utilizados en un determinado radio de acción en el que se encuentra el terminal telefónico que se desea investigar. Es a esta clase de medio técnico al que se refiere el apartado 1 del art. 588 ter l de la LECrim, con respecto a la identificación del aparato que se conecta a la red, aunque a priori pueda parecer sencillo, a parte del medio técnico tiene una gran labor policial detrás, ya que el escáner detectará todos los terminales de la zona, donde serán necesarios varios barridos para ir descartando y mediante la vigilancia ordinaria poder dar con el terminal que se busca[32]. En cuanto al procedimiento ordinario de adquisición de los datos de identificación mediante medios no técnicos, consistirá en la búsqueda de esta información mediante investigación policial, que puede obtener los datos a través de varios medios como listines telefónicos,

[32] RICHARD GONZÁLEZ, M. *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido.* Wolters Kluwer, 2017, Madrid, p. 115.

testigos o confidentes, registros o documentos públicos o privados o mediante la incautación del teléfono[33].

La información albergada en la serie IMSI e IMEI, no puede catalogarse como dato externo integrable en el contenido del derecho al secreto de las comunicaciones, con ellos se desconoce incluso el número telefónico concernido, y las llamadas que pudieran recibirse y efectuarse, y, por supuesto se desconocen las conversaciones por lo que su captación por la Policía Judicial no requiere mandamiento judicial. Para que las operadoras puedan ceder datos sobre IMSI e IMEI sí que será necesaria autorización de la Autoridad judicial, no porque se integren dentro del arco protector del secreto de las comunicaciones sino porque la Ley 25/2007, de 18 de octubre así lo exige[34]. Así se determina en la STS n. º 40/2009, de 28 de enero de 2009, que entiende que no se viola el derecho fundamental al secreto de las comunicaciones por no contener datos de carácter personal de las comunicaciones ni del contenido de las conversaciones.

En este sentido se pronuncia la STS nº 249/2008, de 20 de mayo, que tampoco acepta "que la captura del IMSI por las FCSE suponga una vulneración del derecho al secreto de las comunicaciones, en cuanto, que, por un lado, esa información no permite, por sí sola obtener la identidad de los comunicantes, la titularidad del teléfono móvil o cualesquiera otras circunstancias que lleven a conocer aspectos susceptibles de protección al amparo del artículo 18.3 CE; y que, por otro, la facultad que otorga a las FCSE el art. 22.3 de la LO 15/99, de 13 de diciembre, para la recogida y tratamiento de datos, en el marco de una investigación criminal -nunca con carácter puramente exploratorio- para el esclarecimiento de un delito de especial gravedad, puede considerarse proporcionada y necesaria y, por tanto, ajena a cualquier vulneración de relieve constitucional".

Igualmente la STS 737/2009, de 6 de julio, en relación a la validez de una captura del IMSI realizada por la Policía Judicial, dice que "También existe al respecto una cumplida doctrina de la Sala relativa a que la captura de ese número clave por la policía por sus propios términos para nada lesiona los derechos de privacidad protegidos en el art. 18-3º de la Constitución. Ese número solo permite a la operadora de telefonía conocer el número del teléfono y su titular. Pues bien, para que la operadora ceda esos datos a la policía si hará falta una autorización judicial, y eso es lo que efectuó la

[33] RICHARD GONZÁLEZ, M. *Investigación y …,* op. cit. p. 117-118.
[34] Circular n.º 1/2013 de la FGE, Punto 8.

Guardia Civil como se ha acreditado. En tal sentido SsTS 55/2007; 776/2008; 249/2008 o 630/2008."

En el preámbulo de la ley de modificación de la LECrim se menciona la cesión de los datos desvinculados de los procesos de comunicación concernientes a la titularidad o identificación de un dispositivo electrónico, a los que podrá acceder el Ministerio Fiscal o la Policía Judicial sin necesidad de previa autorización judicial[35]. Se trata de datos de carácter comercial, que no afectan al secreto de las comunicaciones, y permiten al Ministerio Fiscal y a la Policía Judicial avanzar en las investigaciones realizadas en el ejercicio de sus funciones[36].

En la última de las fases, la incriminatoria, se procedería con la intervención de los equipos, del análisis de los mismos y elaboración del atestado, así como la puesta a disposición judicial del autor o autores de los hechos.

Para la intervención de cualquier equipo debe de llevarse a cabo mediante la práctica de la diligencia de entrada y registro domiciliario, la cual requerirá de la oportuna autorización judicial, indicando la finalidad del mismo, que será la intervención de los equipos o dispositivos que pudieran contener indicios racionales de criminalidad.

La técnica para la recogida de cualquier soporte dependerá de cómo se encuentre el equipo, si en funcionamiento o apagado. Ya que en el caso de que se encuentre encendido se realizará una copia de la memoria RAM y comprobar que los discos duros no se encuentre cifrados, que impide futuros accesos.

Este proceso de recogida de soportes digitales varía en función de si el equipo está encendido o apagado. Así, si está encendido se debe realizar una captura de los datos almacenados en la memoria RAM y verificar que las particiones de los discos duros no están cifrados, porque ello impediría que se pueda volver a acceder a ellos en el futuro al no saber las claves. Una vez que se apaga el equipo, se procede a la

[35] FUENTES SORIANO, O., "Comunicaciones telemáticas: práctica y valoración de la prueba", en *El proceso penal. Cuestiones Fundamentales* (Coord. FUENTES SORIANO), Tirant Lo Blanch, Valencia, 2017, pp.281-282.

[36] GUIARD ABASCAL, M.D. Ponencia "La reforma procesal, novedades en la interceptación de las comunicaciones. Obtención, resolución de IP's. Identificación de titulares, terminales o dispositivos de conectividad". Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Dolores%20Guiard%20Abascal.pdf?idFile=559530a2-317c-4eb1-abd0-0594fa7b5210 p.p. 13-18

extracción del disco duro y a su clonación forense, que necesariamente deberá contar con la presencia de los usuarios de los equipos.

El proceso de clonación, es la obtención de una copia exacta, en primer lugar mediante un componente electrónico de bloqueo de escritura que garantiza que no se modifica lo más mínimo. Se han de obtener los códigos llamados *hash* del tipo SHA-256 que determinan que el disco duro original no se ha modificado, a la vez que comprueban que el disco duro clon es una copia exacta del otro. Dichos códigos de comprobación se ejecutan de la siguiente manera: primero se calcula el código de comprobación sobre el disco duro original (antes de realizar el proceso de copia); y luego se realiza sobre el disco duro original y el disco duro clon, después del proceso de copia. Se han obtenido así tres códigos de comprobación que deben ser exactamente iguales[37]. Se deberá garantizar la cadena de custodia, debiendo anotar la marca, modelo y número de serie de los discos duros y después ser etiquetados los dispositivos, para asegurar que estos no han sido manipulados por nadie y que el resultado del análisis corresponde al del contenido. Al obtenerse estas copias habrá que estar a lo dispuesto en el apartado 2 del art. 588 sexies c de la LECrim, donde será necesario que el Letrado de la Administración de Justicia de fe de la operación de copia y de cuáles son los dispositivos que contienen los archivos originales y cuáles donde se copia la información. Una vez realizada la copia, se procederá con el análisis para la obtención de cuantas evidencias se encuentren, que permitan vincular, el usuario con la comisión delictiva para que se pueda determinar su posible responsabilidad criminal. El informe pericial en el que se facilite la información del dispositivo examinado, deberá hacer constar las herramientas informáticas utilizadas para el análisis y las técnicas usadas para averiguar la información[38].

Todas estas prevenciones, tendrán por objeto que estas fuentes probatorias puedan ser válidamente usadas en el proceso judicial.

---

[37] *El proceso de clonación*, disponible en el link: http://www.ondataforensic.com/proceso-de-clonacion.php . Consultado el 15 de abril de 2018.

[38] RICHARD GONZÁLEZ, M. *Investigación y (…)*. op. cit. p. 182-183.

1.5. PRINCIPALES TIPOLOGÍAS DELICTIVAS DE LAS TIC. CIBERCRIMEN

Las principales tipologías delictivas de las TIC, y que investigan la UIT y la GDT, se encuentranrecogidos en el Capítulo II, Títulos I, II, III y VI, del Convenio sobre la Ciberdelincuencia[39].

El Convenio persigue tres objetivos: armonizar el Derecho Penal material, establecer medidas procesales o cautelares adaptadas al medio digital y poner en funcionamiento un régimen rápido y eficaz de cooperación internacional[40].

El término cibercrimen describe y sistematiza nuevas formas de afectación de bienes en el ámbito de las TIC. Pero para que estemos ante un cibercrimen, no bastará que se utilicen las TIC para realizar el comportamiento criminal, sino que se exigirá que tal uso tenga que ver con algún elemento esencial del delito. Por tanto, de forma amplia, podremos definirlo como cualquier comportamiento delictivo realizado en el ciberespacio, entendiendo por el mismo el ámbito virtual de interacción y comunicación personal definido por el uso de las TIC, y relacionado directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio, o comportamientos tradicionalmente ilícitos en los que ahora se llevan a cabo por medio de Internet[41].

Siguiendo la propia estructura del Convenio, podemos clasificar los delitos en cuatro grupos, que son: 1.- delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; 2.- delitos informáticos; 3.- delitos relacionados con el contenido y 4.- delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

En relación con el primero, delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, nos encontraríamos ante delitos descritos en el art. 197 del Código Penal (CP), del descubrimiento y revelación de secretos, en cuanto a la interceptación de las telecomunicaciones en el caso del correo

[39] Convenio nº 185 del Consejo de Europa, más conocido como Convenio de Budapest de 23 de noviembre de 2001, BOE núm. 226, de 17 de septiembre de 2010.
[40] MORÓN LERMA, E. y RODRÍGUEZ PUERTA, M. "Traducción y breve comentario del Convenio sobre Cibercriminalidad", en Revista de derecho y proceso penal. Nº 7, Pamplona, 2002, p. 169.
[41] MIRÓ LLINARES, F. *El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons, 2012, p.p. 40-42.

electrónico o cuando se acceda a datos personales que se encuentren en soportes informáticos, electrónicos o telemáticos[42].

Estamos, por tanto, ante situaciones como el *hacking*, o acceso ilícito a la totalidad o parte de un sistema informático y el *hacker*, como la persona que utiliza determinadas técnicas para acceder, sin la debida autorización, a sistemas informáticos ajenos. Aunque la conducta del *hacker* pueda ser solo intelectual por el hecho de saltar barreras y descubrir vulnerabilidades, cuando se darían respuesta a este tipo de conductas sería con las reformas del CP[43], cuando se darían respuesta a este tipo de conductas.

Otra actividad ilícita es el *cracking*, o la comisión de actos que dañen, borren, deterioren, alteren o supriman datos informáticos por el *cracker*, o aquel que se dedica intencionadamente a eliminar o borrar ficheros o sistemas informáticos, a introducir virus en los mismos, o en general a dañarlos, conductas previstas en el art. 264.1 del CP[44].

Otro delito subsumible en este bloque[45] sería el que sanciona la obstaculización del funcionamiento de un sistema informático mediante la introducción, alteración o supresión de datos informáticos, lo que se ha venido denominando como "sabotaje informático", entre cuyas formas más frecuentes estaría el uso de *malware* o software malicioso, que se lleva a cabo mediante la infección de virus destructivos destinados a dañar, controlar o modificar un sistema informático. Los ataques DoS (*Denial of Services*)[46] consistentes en la utilización de técnicas mediante las cuales se cargan los recursos del ordenador objetivo y así producir la negación del sistema del servidor a otros sistemas informáticos. También el *spamming* o uso de sistemas electrónicos de

[42] Art 197 del CP. 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

[43] LO 5/2010, de 22 de junio y LO 1/2015, de 30 de marzo.

[44] ASENCIO GALLEGO, J.M. "Los delitos informáticos y las medidas de investigación y obtención de pruebas en el Convenio de Budapest sobre la ciberdelincuencia" en *Justicia Penal y nuevas formas de delincuencia.* (Dir. ASENCIO MELLADO J.M, Coord. FERNÁNDEZ LÓPEZ, M.). Ed. Tirant lo Blanch. Valencia. 2017. p.p. 47-49.

[45] art. 264 bis.1 del Código Penal.

[46] MIRÓ LLINARES, F. *El Cibercrimen. …*op. cit. p. 63.

mensajería para enviar mensajes no solicitados (*spam*), especialmente en lo relativo a publicidad, así como su introducción en fotos, blogs o buscados, realizado con ánimo de lucro por los *spammers*[47].

Por último el CP[48] da respuesta a la creación y uso de dispositivos ilegales para la comisión de cualquiera de los delitos del 264 y 264 bis[49].

Respecto del segundo grupo, de delitos informáticos, podemos diferenciar dos categorías diferenciadas. Una primera que son las falsedades informáticas, es decir, la introducción, alteración o supresión de datos informáticos que dé lugar a datos no auténticos (por ejemplo *web spoofing*[50]) y la segunda de fraudes informáticos, como son la introducción, alteración o supresión que causen un perjuicio patrimonial a otra persona (por ejemplo el *phishing* o el *pharming*).

El *phisher* es quien intenta adquirir información confidencial de forma fraudulenta, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica. En el Código Penal no hay ninguna referencia al *phishing*, si bien la mayoría de la jurisprudencia de las Audiencias Provinciales incluye esta conducta en el delito de estafa informática del art. 248.2 a) del CP. Por otra parte el *pharming* es la explotación de una vulnerabilidad en el software de los servidores DNS que permite al atacante redirigir un nombre de dominio[51].

El tercer grupo de clasificación, de delitos relacionados con el contenido, podríamos hablar de cibercrímenes por la ilicitud del contenido. En primer lugar se encuentra la producción, oferta, difusión, adquisición o posesión de pornografía infantil a través de Internet[52]. La pornografía infantil ha pasado por diferentes etapas, que han ido conformando distintos tipos de comportamientos, desde una en la que se empleaban páginas web alojadas en servidores de Internet, en las que el traficante comerciaba con el material pornográfico infantil. Otra en la que se utilizaban los chats y por la que los pedófilos dialogan e intercambian material por email o los grupos de noticias y foros

[47] ASENCIO GALLEGO, J.M. "Los delitos informáticos …op. cit.. p. 52.
[48] Art. 264 ter del Código Penal.
[49] Introducido por la L.O. 1/2015 para tipificar las conductas del art. 6 del Convenio.
[50] El *web spoofing* consiste en la suplantación de una página web.
[51] ASENCIO GALLEGO, J.M. "Justicia Penal…" op. cit. p.p. 54-55.
[52] Delito castigado en el art. 189 del Código Penal.

como medio de comunicación y una última en la que sirven del camuflaje de páginas web no accesibles a través de buscadores[53].

También podríamos incluir situaciones de acoso a menores a través de la red, también conocido como *childgrooming*, que consiste en contactar con menores por medio de las TIC para acercarse a ellos e intentar posteriormente un contacto sexual, delito del art. 183 bis del CP cuando la víctima es menor de 13 años, y que cuando es mayor de esta edad se estaría ante otros tipos penales como amenazas, coacciones, revelación de secretos e incluso pornografía infantil.

También cabría en esta modalidad delictiva el *ciberterrorismo*, que según define DAN VERTON[54] se trata de "la realización de un ataque sorpresa por parte de un grupo terrorista extranjero subnacional con objetivo político utilizando tecnología informáticae Internet para paralizar o desactivar las infraestructuraselectrónicas y físicas de un nación, provocandode este modo la pérdida de servicios críticos, como energíaeléctrica, sistemas de emergencia telefónica, serviciotelefónico, sistemas bancarios, Internet y otros muchos"[55]. Debido a la alarma social y repercusión de este tipo de acciones, fue creado en el año 2003 por parte de la Guardia Civil la Unidad de Ciberterrorismo. En cuanto a las modalidades de ciberterrorismo podemos diferenciar: Incitación y propaganda terrorista (webs de incitación y propaganda), actividades de apoyo informacional (solicitud de financiación, órdenes a las células, adiestramiento y reclutamiento) y ciberataques terroristas directos (Ataques DoD, infecciones de *malware* destructivo e intrusivo)[56].

Por último, encontramos en *cyberhatespeech* o incitación al odio racial en el ciberespacio, delito que no es más que una adaptación al ciberespacio del crimen, ejecutado en el espacio físico en librerías y similares comercios, de difusión de contenidos de odio racial[57].

En cuanto al último de los grupos, de los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, se podría definir como cibercrímenes por la "no autorización en la explotación del contenido" y que se podría

[53] MIRÓ LLINARES, F. *El Cibercrimen* …op. cit. p.p. 109-110.
[54] Dan Verton es periodista especializado en seguridad informática y ex oficial de inteligencia Naval de los Estados Unidos– Washington, D.C. 2003.
[55] SÁNCHEZ MEDERO, G. "El Ciberterrorismo. De la web 2.0 al Internet profundo*".* Revista disponible en http://www.revistasculturales.com/xrevistas/PDF/72/1873.pdf Septiembre, 2015, p.p.100-101
[56] Clasificación realizada por MIRÓ LLINARES, F. *El Cibercrimen. …Op. Cit.* p. 129
[57] MIRÓ LLINARES, F. "*El Cibercrimen. …Op. Cit.* p. 114

clasificar por piratería intelectual, piratería industrial (marcas, diseños) y descubrimiento de secretos de empresa en Internet. La mayoría de estos comportamientos tienen su encaje en el art. 270 del CP, que castiga al que "con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios".

EPIGRAFE 2. PRINCIPALES ACTOS DE INVESTIGACIÓN EN EL CAMPO DE LAS NUEVAS TECNOLOGÍAS

2.1. INTRODUCCIÓN

La promulgación de la LO 13/2015, de 5 de octubre, supuso un importante impulso en la lucha contra la delincuencia en el ciberespacio, regulando por primera vez herramientas de investigación – como señala su exposición de motivos – con las que poder hacer frente a los fenómenos criminales de nuevo cuño, recogiendo en el marco normativo el camino iniciado por la jurisprudencia ante el importante vacío legal que hasta ese momento existía en el ordenamiento. Este apartado pretende recoger algunas de las principales diligencias de investigación tecnológicas de las que la Policía Judicial, y que se servirán para la investigación de la comisión delictiva que se cometa sobre todo mediante el uso de las TIC y teniendo como finalidad la identificación y persecución de su presunto autor. Algunas de las más importantes se encuentran en los siguientes subepígrafes.

2.2. INFILTRACIÓN Y AGENTE ENCUBIERTO EN INTERNET

En primer lugar se hace necesaria dar una definición de lo que sería el agente encubierto en internet. La noción toma como punto de partida el concepto de agente encubierto presencial o habitual, una figura que no es una creación *ex novo*, sino que venía regulado en el art. 282 bis de la LECrim, adaptada al entorno virtual donde actúa y añadiendo dos nuevos apartados al art. 282 bis, el 6 y 7[58].

Como definición de agente encubierto, sería aquel funcionario especializado de la Policía Judicial[59], que cuente con la debida especialización[60] que, con la autorización judicial competente, es designado para introducirse en organizaciones criminales,

[58] RIZO GÓMEZ, B. "La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la LO 13/2015, de 5 de octubre, de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica" en *Justicia Penal y nuevas formas de delincuencia.* (Dir. ASENCIO MELLADO J.M, Coord. FERNÁNDEZ LÓPEZ, M.). Ed. Tirant lo Blanch, Valencia, 2017, p.100.

[59] El apartado 6 del art. 282 bis de la LECrim imposibilita la infiltración realizada por particulares bajo una identidad supuesta, con independencia de los motivos que pudieran motivar su actuación. Lo obtenido por particulares únicamente alcanzará valor de denuncia.

[60] En el caso del agente encubierto en Internet, deberá contar con los conocimientos informáticos necesarios, con carácter general serán miembros de la UIT o GDT.

ocultando su identidad o asumiendo una identidad ficticia de forma temporal, simulando ser parte de ella o estar interesado de los hechos perpetrados por esa organización. Es por tanto herramienta que el legislador ha puesto al servicio de la infiltración policial para identificar a los autores o partícipes, acciones, modus operandi, etc[61].

El funcionario de Policía Judicial designado para realizar las labores de agente encubierto, será escogido por el mando policial y propuesto a la autoridad judicial, y una vez obtenida la autorización judicial, dará comiendo a la infiltración[62] siendo la aceptación del desempeño de tal función de manera voluntaria, no pudiendo imponer la decisión al agente[63].

Vista la figura del agente encubierto, queda patente que respecto al agente encubierto en internet, esta figura no será la misma, la de infiltrarse en una banda criminal organizada, al objeto de integrarse y desarticularla, sino que la infiltración se produce en la red, en canales cerrados de comunicación[64], donde con una identidad también supuesta aunque con sujeción a la ley, se forje una relación de confianza con el delincuente que permita al agente encubierto integrarse en el ámbito de los ciberdelincuentes, con el objetivo de garantizar el éxito de la investigación penal, obtener la información necesaria que permita descubrira la identidad de los autores y relaciones entre ellosy delitos cometidos por ellos[65].

Ante la proliferación de los delitos cometidos a través de internet, el Estado que no podía quedar impasible llevó a cabo la introducción de dos nuevos apartados en la LECrim, mediante la LO 13/2015. El apartado 6 del art. 282 bis dispone que "*El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a. El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y*

[61] VALIÑO CES, A. "La actuación del agente encubierto en los delitos informáticos tras la LO 13/2015" en *El proceso penal. Cuestiones fundamentales.* (Coord. FUENTES SORIANO, O.) Ed. Tirant lo Blanch. Valencia, 2017, p. 378.
[62] RIZO GÓMEZ, B. "Justicia Penal…op. cit.". p.107.
[63] Párrafo 2º del art. 282 bis LECrim.
[64] Las comunicaciones mantenidas en un canal cerrado de comunicación son aquellas que se caracterizan por la expresa voluntad del comunicante de excluir a terceros del proceso de comunicación. Vid STS – sala de lo penal – 20 y 28 de mayo de 2008.
[65] RIZO GÓMEZ, B. "Justicia Penal…op. cit.". p.101.

analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos".

Establece este precepto un escenario para el agente encubierto informático más amplio que el ordinario, pues comprende los delitos contemplados en el art. 588 ter a.

Este precepto faculta al agente encubierto que opera en internet, siempre que medie autorización específica, por un lado intercambiar o enviar archivos de contenido ilícito, medida necesaria para combatir los delitos cometidos por medio de internet y un mal menor, por ejemplo en delitos de pornografía infantil, donde la circulación de archivos no debe integrar la actuación ordinaria del agente encubierto, a pesar que en ocasiones se vuelva imprescindible para el éxito de la investigación[66]. La resolución judicial que autoriza la circulación de los archivos junto con la que habilita al agente encubierto, excluye la posibilidad del delito provocado[67].

Por otro lado, este precepto faculta analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos. Así se pretende identificar de manera inequívoca los archivos ilícitos que se han intercambiado o enviado, realizado a través del *hash*[68]. Esta herramienta es relevante sobre todo en los delitos de pornografía infantil donde mediante el *hash* y por medio de un programa informático se puede determinar donde se encuentran almacenadas dichas fotografías en cualquier parte del mundo.

El apartado 7 del art. 282 bis indica que "*En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio*".

---

[66] RIZO GÓMEZ, B. "Justicia Penal…op. cit.". p.118.

[67] Delito provocado es aquel que aparece cuando la voluntad de delinquir surge en el sujeto, no por su propia y libre decisión, sino como consecuencia de la actividad de otra persona, generalmente un agente o colaborador de las FCS, que guiado por la intención de detener a los sospechosos o de facilitar su detención, provoca a través de su actuación engañosa la ejecución de una conducta delictiva que no había sido planeada ni decidida por aquel, y que de otra forma no hubiera realizado (…). STS – Sala de lo Penal – 13 de mayo de 2014. En el mismo sentido STS – Sala de lo Penal – 6 noviembre de 2013…

[68] Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos). Más información en https://www.genbetadev.com/seguridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales. Consultada el 22 de mayo de 2018.

Con dicha regulación se permite que en una investigación llevada a cabo por el agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de conversaciones que se puedan mantener en los encuentros entre el agente y el investigado, incluso en el interior de un domicilio. Siendo por tanto necesaria una resolución judicial que permita las grabaciones, de manera complementaria, de forma que cualquier limitación de los derechos fundamentales adicional, requiera de una nueva autorización judicial. De esta forma, el agente deberá solicitar la oportuna autorización judicial, siendo el órgano jurisdiccional competente quien valorará la medida solicitada, de acuerdo a los principios de idoneidad, proporcionalidad y necesidad[69].

Interesa poner de manifiesto que la figura del agente encubierto constituye una técnica de investigación extraordinaria, cuando los medios tradicionales de investigación resultan insuficientes. Y es así porque la infiltración policial comporta la restricción de los derechos fundamentales[70], con lo cual existe un procedimiento que hay que seguir para la actuación de un agente encubierto, que se establecen en el mismo art. 282 bis apartado 1 y que suponen una garantía de control para esta figura. Dichos requisitos son los siguientes:

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

- La identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico y social bajo tal identidad.

  El agente infiltrado necesita de una identidad falsa para poder interactuar con los miembros de la organización sin ser descubierto. Esta identidad falsa supone que su actuación se basa en el engaño de los delincuentes, este engaño es un elemento consustancial a la actuación del agente infiltrado

[69] RIZO GÓMEZ, B. "Justicia Penal…op. cit.". p.115.
[70] RIZO GÓMEZ, B. "Justicia Penal…op. cit.". p.102.

proporcionándoles o intercambiando información o archivos con contenido delictivo, que será la que permita cumplir con los objetivos señalados[71].

- La resolución por la que se acuerde deberá consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto. La resolución será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad. Del contenido del art 282 bis.1 2º LECrim se puede llegar a la conclusión de que la identidad verdadera del agente encubierto ha de ser reservada y adoptar las medidas necesarias para mantener su seguridad. Entre las medidas que pueden ser adoptadas destacan las siguientes: a) La resolución en la que figure la identidad verdadera del agente que ha de ser conservada fuera de las actuaciones principales (pieza separada) y adoptándose de forma rigurosa todas las medidas para conservarla. Se baraja la posibilidad de encomendar la custodia con la identidad del agente a la unidad policial competente. b) Conservación de los datos del agente en sobre cerrado custodiado bajo el Letrado de la Administración de Justicia, arts 6 y 7 del RD 1608/2005 de 30 de diciembre, por el que se aprueba el Reglamento Orgánico del Cuerpo de Letrados de la Administración de Justicia. c) Para la designación de la identidad real del agente encubierto en base al artículo 762.7ª LECrim es suficiente con el número de placa o carnet profesional sin hacer constar el nombre y los apellidos del mismo.

- La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente.La información suministrada por el agente y sus actuaciones deberán figurar en una pieza separada[72] declarada secreta por el juez competente. En la pieza especial separada se integrarán la autorización del agente y las diferentes informaciones que este vaya poniendo en conocimiento de quien autorizó su investigación[73] (art. 282 bis 2.3 LECrim).

[71] RIZO GÓMEZ, B. "Justicia Penal…op. cit.". p.102.
[72] STS 975/2007, de 15 noviembre, de 2007.
[73] STS 395/2014, de 13 mayo, de 2014.

No se cuenta únicamente con controles judiciales, sino también policiales, por la figura del controlador o supervisor, responsable directo del agente, siendo una especie de "protector" del funcionario, el cual tendrá contacto con él y deberá saber interpretar las señales de alarma que aproximen su comportamiento al de los delincuentes que investiga. El controlador es el responsable directo de la actuación del funcionario infiltrado; será el que controle sus actividades, marque el camino aseguir, sirva de interlocutor con el resto de investigadores, que pueden tener que participar en la realización de determinadas diligencias, coordinará el dispositivo de seguridad, trasmitirá al agente todo aquello que sea necesario y recogerá deéste la información y fuentes de prueba obtenidas para ponerlas en conocimientodel instructor que autorizó la operación[74].

Por último, es necesario abordar el valor probatorio de la actuación del agente encubierto informático. La información suministrada por el agente encubierto debería ser más un medio de investigación, que una fuente de prueba ya que la finalidad de esta figura es proporcionar datos que permitan avanzar en la investigación de las actividades de la organización criminal[75]. Puede afirmarse, en principio, que su declaración como testigo en la fase de instrucción, no resulta necesaria porque a través de la puesta en conocimiento del Juez de la información que vaya obteniendo ya forma parte del proceso y cumple con su función, de acuerdo con el art. 286 bis 1, 3º LECrim. En consecuencia, existirán situaciones en las que la declaración del agente encubierto resulta imprescindible en el acto del juicio oral, ya que podría constituirse en prueba de cargo para desvirtuar la presunción de inocencia, si así lo valora el tribunal correspondiente. Para ello, el agente deberá prestar declaración en calidad de testigo, conforme al apartado segundo del art. 282 bis LECrim, declaración en la cual relatará aquello que ha sucedido en el curso de la infiltración[76] y sin que sea posible que declare por él un testigo de referencia[77]. Así que si el agente encubierto no ratifica su declaración en el juicio oral, lo dicho en la instrucción fruto de su investigación carecerá de valor probatorio, teniendo el carácter de mera denuncia. En los casos en los que las que el agente encubierto actúe sin la oportuna autorización judicial o en el caso de

[74] DEL POZO PÉREZ M., "El agente encubierto como medio de investigación de la delincuencia organizada en la ley de enjuiciamiento criminal española, en Constitución Europea: aspectos históricos, administrativos y procesales", Criterio Jurídico, Santiago de Cali (Colombia), Nº 6, 2006, p. 282, 301. Disponible en http://revistas.javerianacali.edu.co/index.php/criteriojuridico/article/viewFile/260/1023
[75] STS 975/2007, de 15 noviembre, de 2007
[76] RIZO GÓMEZ, B. "Justicia Penal…Op. Cit.". p.119.
[77] Vid SsTS 395/2014, de 13 de mayo y 104/2011, de 1 de marzo –Sala de lo Penal -

contar con la misma se extralimite en el ejercicio de sus funciones, la prueba obtenida con vulneración de los derechos fundamentales, será nula conforme al art. 11.1 de la LOPJ.

Cuando el agente encubierto declare como testigo se le aplicarán las medidas de la LO 19/1994, de 23 de diciembre de protección de testigos y peritos en causas criminales, art 282 bis.2 in fine LECrim. Estas medidas se adoptarán durante toda la tramitación del procedimiento judicial y de acuerdo con el 2 b de la citada LO que dice que el Juez podrá acordar tales medidas de seguridad que eviten la identificación visual del agente para preservar su imagen y sus derechos.

2.3. TECNOVIGILANCIAS, BALIZAS Y GPS

Una característica de la utilización de las nuevas tecnologías como un instrumento para la investigación de los delitos, es que alguna de las diligencias probatorias puede suponer una injerencia en diferentes aspectos de la privacidad del investigado. Se trata de unas injerencias de la privacidad del investigado, realizadas de una forma que aporta al investigador una reserva total y sigilo mientras se realizan, capaces de ser utilizadas de forma prolongada mientras el investigado ignora que se le están aplicando[78], una de estas técnicas es la tecnovigilancia, que podríamos definir como el sometimiento mediante dispositivos técnicos de control de las actividades de una persona -principalmente-, lugar u objeto preciso en una investigación penal, tanto para poder probar una actividad delictiva pasada (observar quién accede al cuadro robado, por ejemplo), como actual o futura (observar las actividades de los investigados para ver si lo reiteran)[79].

Estas vigilancias tecnológicas, normalmente replicadas en diversos dispositivos de entre los que se obtiene la información, pueden afectar a derechos fundamentales del investigado que, de no aplicarse correctamente puede dar lugar a la nulidad de la prueba, conforme al art. 11.1 LOPJ. Un ejemplo singular de cómo puede llegar a interpretarse la vulneración de derechos fundamentales, sería la STS 329/2016, 20 de

[78] VELASCO NUÑEZ, E. *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*. Sepin, Madrid, 2016, p. 20

[79] VELASCO NUÑEZ, E., "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías", Revista digital El Derecho, 24/02/2011, disponible en: http://www.elderecho.com/tribuna/penal/Novedades-tecnicas-investigacion-vinculadas-tecnologias_11_237430010.html

abril, en la que concluye que observar el interior de una vivienda con algo tan simple como el uso de unos prismáticos por parte de la Policía sin autorización judicial, vulnera el derecho a la inviolabilidad del domicilio, ya que la incursión en un domicilio debe abarcar tanto la entrada física del intruso como la intromisión virtual. La revolución tecnológica ofrece sofisticados instrumentos de intrusión que obligan a una interpretación eficaz del artículo 18.2 de la CE[80].

A nivel probatorio procesal, la información recogida por las tecnovigilancias, normalmente en forma de imágenes y sonidos, pueden servir de auxilio y complemento al testimonio del vigilante, que sin duda serán luego más convincentes[81].

Además de la tecnovigilancia, una de las aplicaciones que hoy en día disponen muchos terminales de telecomunicaciones, es el conocido como GPS[82], de gran utilidad para el investigador ya que permite conocer el posicionamiento, ubicación espacial y temporal del receptor, así como en la obtención de datos como distancias, horarios, itinerarios, etc., donde la obtención de esas informaciones tendrá el objeto de que puedan servir como prueba en el proceso penal, encontrándonos en muchos casos ante datos sensibles de la vida privada que, afectan al art. 18.1 y 18.4 de la CE[83].

Evidentemente se hará necesario intervenir los dispositivos, estando amparada por los arts. 334 y 574 LECrim y exigido a la Policía Judicial 282 y 770.3 LECrim. Tras la intervención del dispositivo que contenga la información, las garantías del proceso exigen su aseguramiento como prueba, mediante la constancia de su cadena de custodia, la extracción de la información para su estudio forense y análisis, que en todo momento debe posibilitar el derecho de defensa[84].

Otro medio de investigación, serían los dispositivos de control remoto conocidos como balizas (o también como vigilancia discreta). Se trata de medios técnicos de geolocalización, que solo permiten conocer la ubicación de las personas, por lo que no afectan,o lo hacen con menor incidencia,a los derechos fundamentales de los presuntos delincuentes que están siendo investigados, pues son mucho menos intrusivas, sin embargo a veces penetran en ámbitos privados (garajes, fincas particulares, etc) donde puede aportar información que va más allá de la que podría aportar el vigilante sin

[80] VELASCO NUÑEZ, E. *Delitos tecnológicos*... op. cit. p. 21
[81] VELASCO NUÑEZ, E., "Novedades técnicas…"op. cit.
[82] Sistema de Posicionamiento Global (Global Positioning System). Para más información http://www.radiofrecuencia.com/tema.php?ID=QUE_SIGNIFICA_GPS
[83] VELASCO NUÑEZ, E. *Delitos tecnológicos*…, op. cit. p. 25
[84] VELASCO NUÑEZ, E. *Delitos tecnológicos*…, op. cit. p. 29.

mandamiento judicial. La privacidad por tanto debe tener doble consideración, una objetiva, lo que socialmente se admite como íntimo según las circunstancias y otra subjetiva, lo que el afectado quiso excluir con su actitud[85].

La jurisprudencia ha ido evolucionando en los supuestos en los que la Policía ha colocado balizas de oficio y sin mandamiento judicial, donde desde el TS en una sentencia de 22 de junio de 2007, en la que indicaba que la colocación policial de una baliza en una embarcación dedicada al tráfico de drogas para su seguimiento en alta mar al no vulnerar ningún derecho fundamental no necesitaba de mandamiento judicial y posteriormente en otra sentencia del propio TS, de 19 de diciembre de 2008, en relación con el sistema de GPS, señala que se podría ver vulnerado el derecho a la intimidad de la persona a la que se geolocaliza, si permitiera "conocer el lugar exacto en el que el comunicante se encontraba" y en estos casos se precisaría en todo caso para el desarrollo de esta diligencia una autorización judicial previa. De modo que si la colocación de la baliza era para una cuestión ocasional o puntual, no exigía mandamiento y era prolongada en el tiempo sí sería necesario, doctrina que pareció consagrarse con la sentencia del TEDH de 2 de septiembre de 2010, caso Azún vs. Alemania[86]. Actualmente, en todo caso obligado por el art. 588 quinquies b) LECrim[87].

En cuanto al empleo de cualquiera de las técnicas vistas, se exige la previa obtención de mandamiento judicial, conforme al art. 588 quinquies b) de la LECrim "cuando concurran acreditadas razones de necesidad y la medida resulte proporcionada, el juez competente podrá autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización", y en dicha autorización, deberá precisarse el medio técnico que va a ser utilizado, de acuerdo con apartado 3 del art. 588 quinquies b) de la LECrim y que la información obtenida, debe ser debidamente custodiada para evitar su utilización indebida (apartado 3 del art. 588 quinquies c) de la LECrim). No será necesaria la previa obtención de mandamiento judicial en los casos de urgencia, en la cual la Policía Judicial procederá y posteriormente deberá solicitar la convalidación judicial (apartado 4 del art. 588 quinquies b).

En cuanto a la duración máxima de las medidas de utilización de dispositivos técnicos de seguimiento y localización, será de tres meses desde la fecha de su

[85] VELASCO NUÑEZ, E. *Delitos tecnológicos*…, op. cit. p.p. 26-27.
[86] VELASCO NUÑEZ, E. *Delitos tecnológicos*…, op. cit. p. 28.
[87] Precepto introducido por la LO 13/2015, de 5 de octubre, de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

autorización, aunque excepcionalmente el Juez podrá acordar prórrogas sucesivas por el mismo o inferior plazo hasta un máximo de 18 meses, siempre que los resultados obtenidos con la medida lo justifiquen (apartado 1º del art. 588 quinquies c) de la LECrim).

Los requisitos para acordar válidamente la medida son escasos. Parece que se exige que "…*concurran acreditadas razones de necesidad y la medida resulte proporcionada*…" (art. 588 quinquies b) LECrim). La Ley no establece unos requisitos mínimos respecto al delito investigado, igual como sucede con otra clase de medidas de investigación electrónica.

Una vez finalice el tiempo de duración de la medida, y siempre que lo solicite el Juez, la Policía Judicial entregará los soportes originales o copias electrónicas auténticas que contengan la información, que como ya se ha mencionado, debe ser debidamente custodiada[88].

Por último señalar que se tratan de tres tipos de diligencias de gran utilidad para permitir confirmar si el investigado ha sido el autor o no del hecho delictivo, que dota de gran discreción en la vigilancia y seguimiento (a diferencia de la vigilancia presencial) y que, tras la última reforma de la LECrim es necesaria la previa autorización judicial.

2.4. TROYANOS. VIRUS ESPÍA

Este acto de investigación lo entenderemos como la utilización, por parte de la Policía Judicial, de los llamados virus "troyanos", en la que se imitan las técnicas malware, pero ahora puestos al servicio de la justicia.

En primer lugar se hace necesario dar una definición de los llamados virustroyanos o espías, tratándose de un programa enmascarado bajo otra denominación, que, una vez abierto, puede desplegar su contenido en el ordenador del investigado sin su conocimiento y con ello obtener la oportuna información de su actividad delictiva a través de su terminal[89].

[88] MUERZA ESPARZA, J. *Las reformas procesales penales de 2015*. Thomson Reuters. Navarra. 2015, p. 176.
[89] VELASCO NUÑEZ, E., "Novedades técnicas… op. cit.

Por tanto mediante esta técnica de investigación, se introducirá de forma furtiva el troyano en el ordenador del investigado[90], con el propósito de obtener pruebas y vigilar su actividad, sin su consentimiento ni conocimiento, pero con la oportuna autorización judicial, de acuerdo con el art. 588 septies a) LECrim, de forma que se consiga cuantos datos se almacenen en el disco duro o memoria del ordenador, así como todas las comunicaciones que no salgan a la Red, el tráfico de entrada y salida de sus telecomunicaciones y del historial de las web visitadas, de forma se copiarían los datos seleccionados para su análisis[91].

En consecuencia, se podría decir que supone monitorizar la información del ordenador, smartphone, tableta, etc. del investigado y que a su vez duplicaría esta información, de tal forma que se evite que el investigado pueda alterar o destruir los datos. Y, por tanto, el objeto de la intervención del ordenador con el virus troyano, es tener conocimiento de toda la información contenida y tratada en el soporte por el investigado, y las circunstancias en las que son realizadas, ya se encuentre en el propio equipo o en los servidores que este visite – pudiendo afectar a la privacidad informática conforme al art. 18.4 CE y las telecomunicaciones electrónicas que realice, - y en este caso al 18.3 CE[92].

Esta herramienta se puede contar de entre las más eficaces, en primer lugar por la discreción en la captación de información, donde no es necesaria la intermediación de ninguna empresa proveedora de los servicios de internet, en segundo exige menos investigadores que cualquier otra técnica de tecnovigilancia y capta más información sobre la actividad del investigado, en tercero porque cuenta con una gran movilidad ya que opera a través de internet, donde los posibles desplazamientos al extranjero del investigado no condicione la eficacia de la investigación. Ello no obstante, no está exenta de inconvenientes, ya que es posible su detección por programas antivirus, a no ser que se solicite colaboración a los proveedores de antivirus, de acuerdo con el art.

[90] Diversas fuentes policiales, enuncian entre otras formas de introducción:
- Mediante una página web manipulada para que el sospechoso acceda a la página y así se descargue el programa, pero con el riesgo de que otros usuarios se contagien.
- Mediante una página web con contenidos delictivos de señuelo, de manera que el virus alojado en esa página se instale en el ordenador del visitante, o descargue alguno de sus contenidos. Pero tiene como inconveniente que evoca la figura del delito provocado.
- Con un email que contenga un "gusano oculto", con el problema de que se infecten los correos de la lista de contactos del destinatario.
- La más eficaz sería con la inserción del mismo en un USB, con el problema para los investigadores tuvieran que sustraerle un USB al sospechoso y devolvérselo infectado.

[91] VELASCO NUÑEZ, E. *Delitos tecnológicos*…, op. cit. p. 33.

[92] VELASCO NUÑEZ, E. *Delitos tecnológicos*…, op. cit. p. 34.

588 septies b) LECrim, que para su instalación es necesaria conexión a internet para poder alojar el troyano[93].

En cuanto a la duración de la medida, habrá que estar a lo dispuesto en el art. 588 septies c), que dispone que "la medida tendrá una duración máxima de un mes, prorrogable por iguales períodos hasta un máximo de tres meses". Sin duda esta limitación temporal puede llevar a la reflexión de los razonamientos que motivaron al legislador a la adopción de dicho espacio de tiempo. La medida, es tanto como la práctica monitorización de la actividad del investigado, ya sea a través de su ordenador o de su smartphone, donde hoy en día los aspectos más privados de la persona suelen estar alojados en este tipo de dispositivos. Sin duda, cuanto menos, cabe preguntarse si dicha privacidad está siendo lesionada, donde como mínimo la Policía Judicial tendrá conocimiento de aspectos de la vida privada que nada tendrán que ver con el objeto de la investigación.

Por último, mencionar que al introducir troyanos en el dispositivo del sospechoso, surgen problemas jurídicos que la práctica procesal deberá resolver, alguno de los cuales son los posibles motivos espurios de los investigadores; el análisis de las prácticas a las que conduce el uso cotidiano de las nuevas tecnologías y saber hasta dónde debe alcanzar la privacidad, intimidad y vida privada; la protección de la información automatizada que a diario se emiten a múltiples entidades para fines distintos para los que se han cedido; una aclaración legal de estas técnicas invisibles, por ser intrusivas, imperceptibles e indetectables, debiendo de excluirse en todo caso su uso por parte de particulares y sólo para la protección de intereses importantes; la aportación al proceso de los resultados de la forma más fiable posible y que se garantice la procedencia, inalterabilidad y autenticidad, correcto almacenamiento y custodia[94]. Quizás una solución de aplicación más temprana que el desarrollo de la práctica procesal, sería establecer unos protocolos de actuación y directrices adecuadas dirigidas sobre todo a la Policía Judicial, de forma que se puedan evitar ulteriores problemas.

[93] VELASCO NUÑEZ, E. *Delitos tecnológicos*…, op. cit. p. 35.
[94] VELASCO NUÑEZ, E. *Delitos tecnológicos*…, op. cit. p.p. 37-38.

2.5. DRONES

Un dron es un vehículo aéreo no tripulado, por eso también se le puede llamar VANT, que sería la abreviatura de vehículo aéreo no tripulado en español. Los drones pueden ser controlados por pilotos desde el suelo o cada vez más, de manera autónoma después de ser programados con anterioridad. El empleo cada vez mayor de los drones, ha provocado un incremento en cuanto a lostiposexistentes, contando con diversidad de modelos[95]. Esta amplia variedad, permite su uso en multitud de situaciones de todo tipo, ya que cuentan con amplias posibilidades gracias a la posibilidad de tener incorporadas cámaras, micrófonos, localizadores, etc. y convertirse así en una buena herramienta de investigación penal, junto con los métodos ya existentes y el resto de medidas de investigación tecnológica introducidas en la reciente LO 13/2015.

Las principales ventajas que reportan son su fácil manejabilidad, ausencia de peligro de quienes los controlan, y sus escasos costes en relación con otras alternativas, provocando que los drones desbanquen a los helicópteros y vehículos similares en ciertos ámbitos, al ser una respuesta más adecuada a determinadas situaciones.

Sin embargo, es fundamental la regulación del uso de los mismos con el objetivo de evitar su utilización para fines ilícitos tan distintos que van desde la injerencia en la esfera privada de la persona, hasta los más graves -como los producidos en Tokio cuando fue encontrado en la terraza de un edificio del gobierno un dron equipado con una cámara y un líquido radioactivo-**,** y también impedir que personas que no cuenten con la suficiente competencia los utilicen y se eviten posibles accidentes, de modo que no se manejen estos aparatos cuando exista un riesgo para la seguridad de los demás[96].

Los drones atienden a múltiples modalidades debido a sus diversas características. Una clasificación adecuada podría ser en función del uso para el que estén destinados, siendo ésta la distribución más interesante en relación con su marco legal. Así, podemos clasificarlos en dos grandes grupos: drones para uso militar y para uso civil. A su vez, dentro de los de uso civil, estarán los destinados a los servicios públicos de las administraciones (dentro de las que encontramos la videovigilancia por las FCS), para fines comerciales y, finalmente, para uso particular.

---

[95] Para más información, vid. http://www.areatecnologia.com/aparatos-electronicos/drones.html

[96] ¿Qué es un drone? ¿Para qué sirve?.https://tecnologia-informatica.com/que-es-drone-para-que-sirve-comprar/ Consultado el 10 de junio de 2018.

Como se puede comprobar, el uso que se puede hacer de los drones es muy variado, por ello análisis se va centrar en analizar únicamente en el empleo de drones con fines de seguridad por parte de las FCS.

Los drones se han popularizado hasta tal punto entre los cuerpos de policía, que incluso ha llegado a las administraciones locales[97], ya que es un sistema de vigilancia poco visible y pueden permanecer en el aire durante mucho tiempo. Los drones permiten así hacer fotografías aéreas con alta definición, ya que están provistos de potentes cámaras y sistemas de rastreo avanzados. No sólo sirven para captar y almacenar imágenes, sino que pueden llegar incluso a hackear redes de WiFi o a interceptar comunicaciones civiles. Igualmente, cada vez hay más drones con dispositivos de reconocimiento facial y captación de imágenes térmicas que ayudan a los entes policiales a detectar criminales. Estos sensores permiten monitorizar a los sospechosos cada vez con mayor precisión[98].

Teniendo en cuenta todo lo anterior, se pone de manifiesto que suponen una intrusión en los derechos fundamentales de la persona, desde la privacidad, el derecho al secreto de las comunicaciones o la inviolabilidad del domicilio, pues cuentan con herramientas suficientes para grabar personas en sus casas o lugares de trabajo. Asimismo es posible equiparles con herramientas de reconocimiento facial o biométrico lo que hace posible monitorizar y seguir individuos basándose en la altura, edad, sexo o raza, con las implicaciones que supone para la privacidad[99].

En cuanto a su normativa, empezando en el seno de la UE, desde el año 2004 la UE dispone de competencias para gestionar el espacio aéreo de los Estados miembros. En este contexto, el mercado de los drones en territorio europeo ha ido aumentando año tras año. Se sabe que al menos dieciséis Estados miembros de la UE utilizan ya dronespara fines militares y policiales. Desde 2009 con el Tratado de Lisboa la UE adquiere nuevas competencias en el ámbito de la seguridad interior de la UE. Bajo el nuevo tratado, la Comisión Europea anunció su voluntad de introducir legislación al

---

97 Vid. https://www.aerotendencias.com/uav/34309-la-policia-local-de-benidorm-utiliza-un-drone-para-vigilar-playas-y-el-entorno-rural/

98 BLASI, C., "El empleo emergente de drones con fines policiales en la Unión Europea: avances y limitaciones", editado por Grupo de Estudios en Seguridad Internacional (GESI), Granada, 2014. Disponible en: http://www.seguridadinternacional.es/?q=es/content/el-empleo-emergente-de-drones-con-fines-policiales-en-la-uni%C3%B3n-europea-avances-y Consultado el 10 de junio de 2018.

99 ACED FÉLEZ, E., "Drones: una nueva era de la vigilancia y de la privacidad", *Revista Red Seguridad*, disponible en: http://www.redseguridad.com/especialidades-tic/proteccion-de-datos/drones-una-nueva-era-de-la-vigilancia-y-de-la-privacidad Consultado el 10 de junio de 2018.

respecto para fines tanto comerciales como de seguridad. Así, en septiembre de 2012, ésta publicó un informe llamado "Hacia una estrategia europea para el desarrollo de aplicaciones civiles en el uso de VANT", donde expresaba la necesidad de regular el funcionamiento de estos sistemas. Sin embargo, las competencias de seguridad siguen recayendo sobre los Estados miembros en su mayor parte. Por ello, los drones usado con fines policiales quedan aún excluidos de cualquier normativa europea actual[100]. Bruselas quiere crear en 2019 un espacio europeo controlado para drones.

Ya a nivel interno, acudiremos en primer lugar al RD 1036/2017, de 15 de diciembre por el que se regula la utilización civil de las aeronaves pilotadas por control remoto. Aunque regula la utilización de drones por particulares con fines recreativos, también se incorporan preceptos para el uso de estos dispositivos por la Policía Judicial, y desde la perspectiva de la LO 13/2015 de reforma de la LECrim, establece su posible uso como una diligencia de investigación tecnológica. Ambas normativas desembocan en una realidad procesal, por la que la finalidad del uso de drones será la captación de pruebas audiovisuales, que deberán ser obtenidas con respeto a los derechos de los investigadosy aportadas al proceso con todas las garantías[101].

Con el actual RD 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, elimina muchas de las restricciones que establecía la Ley 18/2014 y que limitaba en exceso las posibilidades de uso de estos dispositivos, y se esclarecen cuestiones antes consideradas ambiguas.

Respecto al ámbito de aplicación del RD el mismo se limita a "aeronaves y elementos que configuran el sistema de aeronave pilotada por control remoto", quedando fuera los dispositivos automatizados. Al margen del manejo por civiles para fines lúdicos con una serie de restricciones, entran dentro del ámbito de aplicación aquellos aparatos cuya masa máxima al despegue no sea superior a 150 kg, salvo aquellos que sean manejados por Policía Judicial para operaciones relacionadas con el control de aduanas, extinción de incendios o la búsqueda y salvamento de personas.

---

[100] BLASI, C., "El empleo emergente de drones con fines policiales (…)" op cit.

[101] BUENO DE MATA, F. "La utilización de drones como diligencia de investigación tecnológica: consecuencias probatorias, *Diario La Ley*, nº 16, Sección Ciberderecho, WoltersKluwer, 20 de Marzo de 2018, p.1. Disponible en: http://laleydigital.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAiMzU0MLU7Wy1KLizPw8WyMDQwsDYyMDkEBmWqVLfnJIZUGqbVpiTnGqWmaxY0FBUX5ZagpEnamBuYGliQUAC2xxw00AAAA%3DWKE

En cuanto al uso del dron como diligencia de investigación policial en la LO 13/2015 no hay ninguna mención a los mismos. Por lo tanto, se debe acudir al bloque de "utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes ", en concreto al art. 588 quinquies a) que permite a "La Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos", y donde la Policía Judicial entregará al juez los soportes originales o copias electrónicas auténticas que contengan la información recogida cuando éste se lo solicite y, en todo caso, cuando terminen las investigaciones", conforme al apartado segundo de la letra c) y en el apartado tercero establece que se garantice la cadena de custodia "la información obtenida a través de los dispositivos técnicos de seguimiento y localización a los que se refieren los artículos anteriores deberá ser debidamente custodiada para evitar su utilización indebida".

Con todo ello la normativa permite utilizar un dron como medidas de investigación policial y posteriormente aportarlo como prueba al proceso a fin de reproducir su contenido durante la vista oral. Igualmente, esta normativa se complementa con el RD 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, que dota de un marco de actuación más puntual para su utilización en operaciones de policía de las FCS, funciones de guardacostas y servicios de aduanas, misiones de vigilancia del tránsito viario, y operaciones del Centro Nacional de Inteligencia, así lo especifica en su art. 2 que se aplicara a las aeronaves pilotadas por control remoto "cualquiera que sea su masa máxima al despegue, que efectúen actividades de aduanas, policía, búsqueda y salvamento, lucha contraincendios, guardacostas"[102].

La finalidad de la utilización del dron como diligencia de investigación tecnológica es la de captación de imágenes o vídeos y, por tanto, será una herramienta para la obtención de pruebas electrónicas que puedan atribuir la autoría del crimen a un determinado autor. Y a este respecto, hay que hacer referencia a la obtención de las imágenes captadas con el dron, con el fin de que no se vulneren derechos fundamentales del investigado[103]. Aclarar que las grabaciones realizadas por drones en espacios

[102] BUENO DE MATA, F. "La utilización de drones…" op. cit. p. 5.
[103] Por ejemplo, no será posible la grabación con un dron del interior de un domicilio.

abiertos por personal vinculado a las Administraciones Públicas, no se verían afectados en ningún caso la privacidad ni por supuesto el derecho a la intimidad, el derecho a las comunicaciones o el derecho a la inviolabilidad en domicilio, todo ello de acuerdo tanto del RD como de la LO 13/2015.

Partiendo de que no se va a incurrir en la obtención de pruebas violando derechos fundamentales del investigado, nos encontramos ante la posibilidad de alteración o manipulación del material electrónico desde que es captado hasta que es practicado en sede judicial. Para ello, es necesario en estos casos preservar fielmente la cadena de custodia de la prueba a través de técnicas de aseguramiento informatizadas, como las técnicas de "sellado de tiempo" o encriptación[104]. Aún así, es urgente la promulgación de una Directiva en materia de obtención de pruebas electrónicas en terreno europeo para una posterior transposición a derecho nacional, donde se establezcan unas pautas mínimas que fueran implementadas[105].

Serán las FCS los principales sujetos que obtienen este tipo de evidencias y que posteriormente deberán trasladarlas al proceso y tendrán la responsabilidad antes de aportarlo al proceso, de ser los encargados de, o bien custodiar la prueba y realizar una tarea de aseguramiento,o bien controlar que un tercero lo haga, si no son ellos los que propiamente aportan la prueba. Así, el art. 588 octies, al hablar de conservación de datos de las diligencias de investigación tecnológica dice que "El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente (...) El requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, quedando sujeto a la responsabilidad descrita en el apartado 3 del artículo 588 ter e".

Respecto a la aportación de las imágenes, vídeos y fotografías realizadas por el dron o los informes periciales vinculados a este último, según este RD debemos otorgarles el tratamiento de archivos electrónicos, por lo que deberán ir acompañados de

[104] La información obtenida se cristaliza en un determinado momento a través de una serie de parámetros alfanuméricos quedando impertérrita hasta su práctica.
[105] BUENO DE MATA, F. "La utilización de drones…" op. cit. p. 9.

un formulario normalizado y homogéneo con el detalle o índice comprensivo del número, orden y descripción somera del contenido de cada uno de los documentos[106].

[106] BUENO DE MATA, F. "La utilización de drones…" op. cit. p. 12.

CONCLUSIONES

Tras la elaboración del presente Trabajo Fin de Grado sobre las Fuerzas y Cuerpos de Seguridad del Estado, actuando como Policía Judicial y de los actos de investigación que se están utilizando en la investigación de los delitos de las TIC, se concluye:

1. Los delitos cometidos a través de Internet, presentan una naturaleza y unas características especiales, que facilitan su comisión e impunidad a una pluralidad de personas tanto físicas como jurídicas, independientemente del lugar donde estas se encuentren y con grave afectación a bienes jurídicos protegidos. Estas características son su rapidez en su comisión, el anonimato que otorga la Red y con un alcance internacional y masivo.

2. Por las singulares características de estos delitos y por el medio en el que se producen, ha sido necesario contar con grupos especializados dentro de las Fuerzas y Cuerpos de Seguridad del Estado de funcionarios con conocimientos y formación específica en este campo.

3. Los actos de investigación que deben llevar a cabo estos profesionales, en su labor como Policía Judicial para la averiguación del delito cometido a través de las TIC y del descubrimiento de los delincuentes, afectan a derechos fundamentales del investigado del art. 18 de la CE, como el derecho a la intimidad o al secreto de las comunicaciones, motivo por el que deberá contar con la oportuna autorización judicial y limitación temporal de la medida, con motivo de la reciente modificación de la LECrim, por parte de la LO 13/2015, de 5 de octubre.

4. La particular característica de la internacionalidad de estos delitos y de sus autores, hace necesario un avance en cooperación, coordinación y armonización de los países implicados, tanto a nivel legislativo, policial y judicial, debido a que actualmente no se cuentan con mecanismos ágiles y eficaces para la persecución internacional.

5. Aún quedan cuestiones que la práctica procesal deberá resolver, ya que debido a la reciente reforma de la LECrim y al tiempo que los procesos tardan en llegar a las instancias superiores, apenas hay jurisprudencia desde la entrada en vigor de la LO 13/2015, de 5 de octubre, que haya interpretado interrogantes tales como la adaptación de la reforma a la luz del respeto a los DDFF.

BIBLIOGRAFÍA

ACED FÉLEZ, E., "Drones: una nueva era de la vigilancia y de la privacidad", *Revista Red Seguridad,* disponible en: http://www.redseguridad.com/especialidades-tic/proteccion-de-datos/drones-una-nueva-era-de-la-vigilancia-y-de-la-privacidad

ASENCIO GALLEGO, J.M. "Los delitos informáticos y las medidas de investigación y obtención de pruebas en el Convenio de Budapest sobre la ciberdelincuencia" en *Justicia Penal y nuevas formas de delincuencia.* (Dir. ASENCIO MELLADO J.M, Coord. FERNÁNDEZ LÓPEZ, M.). Ed. Tirant lo Blanch. Valencia. 2017.

BLASI, C., "El empleo emergente de drones con fines policiales en la Unión Europea: avances y limitaciones", editado por Grupo de Estudios en Seguridad Internacional (GESI), Granada, 2014. Disponible en: http://www.seguridadinternacional.es/?q=es/content/el-empleo-emergente-de-drones-con-fines-policiales-en-la-uni%C3%B3n-europea-avances-y

BUENO DE MATA, F. "La utilización de drones como diligencia de investigación tecnológica: consecuencias probatorias, *Diario La Ley*, nº 16, Sección Ciberderecho, WoltersKluwer, 20 de Marzo de 2018. Disponible en: http://laleydigital.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAiMzU0MLU7Wy1KLizPw8WyMDQwsDYyMDkEBmWqVLfnJIZUGqbVpiTnGqWmaxY0FBUX5ZagpEnamBuYGliQUAC2xxw00AAAA%3DWKE

DEL POZO PÉREZ M., "El agente encubierto como medio de investigación de la delincuencia organizada en la ley de enjuiciamiento criminal española, en Constitución Europea: aspectos históricos, administrativos y procesales", Criterio Jurídico, Santiago de Cali (Colombia), Nº 6, 2006, p. 282, 301. Disponible en http://revistas.javerianacali.edu.co/index.php/criteriojuridico/article/viewFile/260/1023

FUENTES SORIANO, O., "Comunicaciones telemáticas: práctica y valoración de la prueba", en *El proceso penal. Cuestiones Fundamentales* (Coord. FUENTES SORIANO), Tirant Lo Blanch, Valencia, 2017.

GUIARD ABASCAL, M.D. Ponencia "La reforma procesal, novedades en la interceptación de las comunicaciones. Obtención, resolución de IP's. Identificación de titulares, terminales o dispositivos de conectividad". Disponible en:

https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Dolores%20Guiard%20Abascal.pdf?idFile=559530a2-317c-4eb1-abd0-0594fa7b5210

LORENZANA GONZÁLEZ, C. "Ponencia: La Investigación de delitos telemáticos por la Guardia Civil, y sus capacidades al servicio del Ministerio Fiscal". p.4. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20escrita%20Sr%20Lorenzana.pdf?idFile=e14972b0-5d5a-40d6-8940-f1ef8152c3f9

MIRÓ LLINARES, F. *El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons, 2012.

MORÓN LERMA, E. y RODRÍGUEZ PUERTA, M. "Traducción y breve comentario del Convenio sobre Cibercriminalidad", en Revista de derecho y proceso penal. Nº 7, Pamplona, 2002.

MUERZA ESPARZA, J. *Las reformas procesales penales de 2015*. Thomson Reuters. Navarra. 2015.

NÚÑEZ IZQUIERDO, F. "La policía judicial. El auxilio con la administración de justicia en la investigación criminal". http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4759-la-policia-judicial-el-auxilio-con-la-administracion-de-justicia-en-la-investigacion-criminal/

ORTIZ PRADILLO J.C., *La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, ed. Fundación Alternativas, disponible en: http://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf Madrid, 2013.

Revista Red Seguridad nº 072, Primer trimestre 2016, Bormart S.A. pp. 8-9. Disponible en: http://www.redseguridad.com/revistas/red/072/index.html#8

RICHARD GONZÁLEZ, M. *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido.* Wolters Kluwer, 2017, Madrid.

RIZO GÓMEZ, B. "La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la LO 13/2015, de 5 de octubre, de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las

medidas de investigación tecnológica" en *Justicia Penal y nuevas formas de delincuencia*. (Dir. ASENCIO MELLADO J.M, Coord. FERNÁNDEZ LÓPEZ, M.). Ed. Tirant lo Blanch, Valencia, 2017,

SÁNCHEZ MEDERO, G. "El Ciberterrorismo. De la web 2.0 al Internet profundo*"*. Revista disponible en http://www.revistasculturales.com/xrevistas/PDF/72/1873.pdf Septiembre, 2015.

VALIÑO CES, A. "La actuación del agente encubierto en los delitos informáticos tras la LO 13/2015" en *El proceso penal. Cuestiones fundamentales.* (Coord. FUENTES SORIANO, O.) Ed. Tirant lo Blanch. Valencia, 2017.

VELASCO NUÑEZ, E. *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*. Sepin, Madrid, 2016.

VELASCO NUÑEZ, E., "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías", Revista digital El Derecho, 24/02/2011, disponible en: http://www.elderecho.com/tribuna/penal/Novedades-tecnicas-investigacion-vinculadas-tecnologias_11_237430010.html