VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO FIN DE GRADO

Grado en Derecho

Departamento: Derecho Administrativo, Financiero y Procesal

Área de conocimiento: Derecho Procesal

Curso 2014/2015

DILIGENCIAS DE INVESTIGACIÓN Y NUEVAS TECNOLOGÍAS

MARÍA TERESA PASCUAL MARTÍN

Tutor: FEDERICO BUENO DE MATA

JUNIO 2015.

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO FIN DE GRADO

Grado en Derecho

Curso 2014/2015

DILIGENCIAS DE INVESTIGACIÓN Y NUEVAS TECNOLOGÍAS

MARÍA TERESA PASCUAL MARTÍN

Tutor: FEDERICO BUENO DE MATA

JUNIO 2015.

FIRMA DEL ALUMNO **FIRMA DEL TUTOR**

MARÍA TERESA PASCUAL MARTÍN **FEDERICO BUENO DE MATA**

TRABAJO FIN DE GRADO

GRADO EN DERECHO

Departamento: Derecho Administrativo, Financiero y Procesal

Área de conocimiento: Derecho Procesal

Curso 2014/2015

TÍTULO:

DILIGENCIAS DE INVESTIGACIÓN Y NUEVAS TECNOLOGÍAS

TITLE:

PROCEEDINGS OF RESEARCH AND NEW TECHNOLOGIES

Nombre del/la estudiante: MARÍA TERESA PASCUAL MARTÍN
e-mail del/a estudiante: mayte.mov_12@hotmail.com

Tutor/a: FEDERICO BUENO DE MATA

RESUMEN:

En el trabajo se analizan las principales diligencias de investigación policial que han surgido para combatir los delitos cometidos a través de las nuevas tecnologías, diligencias tales como la prueba del ADN, la biometría, las entregas vigiladas a través de Internet, la tecnovigilancia, balizas y GPS, el agente encubierto en Internet, los virus espía, los drones y la P300. La nota común de todas estas diligencias es la falta de regulación legal, que se intenta paliar con la aprobación del Proyecto de Ley Orgánica, presentado por el Consejo de Ministros el 13 de Marzo de 2015. Asimismo, se hace referencia a los dos grupos especializados de las Fuerzas y Cuerpos de Seguridad del Estado y a los concretos protocolos de actuación que desarrollan para investigar estos delitos, destacando el sistema informático de interceptación de las telecomunicaciones, SITEL, como uno de los avances tecnológicos más utilizado en la lucha contra el cibercrimen.

PALABRAS CLAVE: Diligencias de investigación policial, nuevas tecnologías, cibercrimen.

ABSTRACT

At work, we analyze the main diligences of police investigation that have emerged to combat criminal acts committed through the new technologies. Proceedings such as DNA testing, biometry, controlled deliveries via the Internet, technovigilance, beacons and GPS, undercover agent on the Internet, spy virus, drones and P300.

The common note of all these diligence is the lack of legal regulation, which it is trying to compensate with the approval of the Organic Law Project presented by the Council of Ministers on March 13, 2015.

It also refers to the two specialized groups of the Security Forces of the State and the specific protocols that they developed to investigate these crimes, highlighting SITEL, as one of the most used technological advances in the fight against cybercrime.

KEYWORDS: Diligences of police investigation, new technologies, cybercrime.

ÍNDICE

ABREVIATURAS

ADN: Ácido desoxirribonucleico

Art/s: Artículo/s

BDEF: Brigada de Delincuencia Económica y Financiera

BIT: Brigada de Investigación Tecnológica

CE: Constitución Española

CP: Código Penal

DEI: Departamento de Electrónica e Informática

DoS: Denial of Service

DDoS: Distributed Denial of Service

EDITE,s: Equipos de Investigación Tecnológica

GDI: Grupo de Delitos Informáticos

GDT: Grupo de Delitos Telemáticos

GPS: Sistema de Posicionamiento Global

I+D: Investigación y Desarrollo

IMSI: Identidad Internacional de Suscriptor Móvil

IMEI: Identidad Internacional de Equipos Móviles

ISFG: Sociedad Internacional de Genética Forense

LECrim: Ley de Enjuiciamiento Criminal (1882)

LO: Ley Orgánica

P2P: Red entre iguales

SITEL: Sistema Integrado de Interceptación Telefónica

STS/SSTS: Sentencia/s del Tribunal Supremo

TFG: Trabajo Fin de Grado

TICs: Tecnologías de la Información y Comunicación

TS: Tribunal Supremo

UDEF: Unidad de Delincuencia Económica y Financiera.

UIT: Unidad de Investigación Tecnológica

VANT: Vehículo Aéreo No Tripulado

1. INTRODUCCIÓN

El presente Trabajo de Fin de Grado pretende analizar las diligencias policiales que se han desarrollado y se están desarrollando para combatir los delitos surgidos con la aparición de las nuevas tecnologías, haciendo mención a las Fuerzas y Cuerpos de Seguridad del Estado que se dedican a ello y a los protocolos de actuación que desarrollan para investigar estos delitos.

Para poder averiguar si ha sucedido o no un hecho punible, en qué circunstancias y quien lo ha cometido, hay que efectuar una serie de actividades que pretendan esta finalidad, estas actividades son las diligencias de investigación que lleva a cabo la Policía Judicial y por eso también se conocen como diligencias policiales[1]. Estas diligencias de investigación tradicionales con las que cuenta la Policía Judicial se contienen en el Título V de la LECrim., arts. 326 a 485. Asimismo encontramos otras diligencias en el art. 282 bis que regula la figura del agente encubierto en el terreno físico como otra diligencia policial, así como en el art. 263 bis que regula la entrega vigilada.

Ahora bien, hay que tener en cuenta como han afectado a estas diligencias las nuevas tecnologías. Así las cosas, los grandes avances que en los últimos tiempos se han producido en materia informática han llevado a una auténtica revolución tecnológica que nos permite hablar del entorno digital del individuo, esto es, usamos la tecnología para comunicarnos, para educar, sanar, fabricar, jugar, pero también para delinquir, pues no siempre se hace un uso responsable de Internet.

Se están utilizando las nuevas tecnologías para delinquir porque presentan unas características muy favorables para los autores de los ciberataques, y ello debido al bajo coste que presentan, pues las herramientas que utilizan los atacantes pueden obtenerse gratuitamente o a un coste muy reducido; debido también a la ubicuidad, pues para desarrollar los ataques es independiente la localización de los agresores; y, debido, en último lugar, a que tienen un reducido riesgo para los atacantes, pues la facilidad de ocultación hace que no sea fácil atribuir la comisión de un ciberataque a su verdadero autor o autores. Considerando todo esto unido a que no existe una regulación en la

[1] En este sentido el art. 282 de la LECrim señala que la Policía Judicial tiene por objeto, y será obligación de todos los que la componen, practicar, según sus atribuciones, las diligencias necesarias para comprobar los delitos que se cometan en su territorio o demarcación 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.

materia, se pone de manifiesto la dificultad para la persecución de estos delitos. Por último hay que destacar igualmente la efectividad de estos medios, pues debido a la falta de regulación, casi siempre alcanzan los objetivos que persiguen.

Ahora bien, hay que tener en cuenta que al igual que se usan las nuevas tecnologías para delinquir, esta misma tecnología se está utilizando en la investigación de los delitos por parte de las Fuerzas y Cuerpos de Seguridad del Estado para resolver los casos. Ya no les basta simplemente con el arma de fuego, las esposas y el bloc para tomar notas, sino que en la actualidad se requiere el empleo de la informática para investigar los delitos que se cometen utilizando las nuevas tecnologías. Los avances tecnológicos constituyen una herramienta de trabajo tanto para la policía científica en su labor de análisis de huellas y rastros en el laboratorio, como en el ámbito de la vigilancia, a través de diligencias como la videovigilancia mediante cámaras IP con activación remota, el agente encubierto en Internet, los drones, los sistemas de imágenes térmicas, de visión nocturna o por satélite, los equipos de reconocimiento biométrico del rostro de personas, sus iris, así como el uso de la tecnología GPS para conocer la ubicación geográfica exacta de un concreto dispositivo[2].

En muchas ocasiones imputar determinados delitos a sus presuntos autores resulta una tarea difícil, y más en el plano virtual donde el anonimato que ofrece la red complica esta tarea. En consecuencia, se plantea si para el descubrimiento de estos delitos se pueden utilizar algunas de las técnicas informáticas usadas para delinquir como técnicas a su vez de investigación de este tipo de delincuencia, así como otras hasta la fecha desconocidas que empiezan a surgir por los propios avances de las tecnologías[3].

Hay que hacer en este punto una mención obligada al Proyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, presentado por el Consejo de Ministros el 13 de Marzo de 2015, que en su exposición de motivos menciona que pretende la regulación de las medidas de investigación tecnológica en el ámbito de los derechos a la intimidad, al secreto de las

[2] ORTIZ PRADILLO, J.C., "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar el delito*, ed. La Ley, Madrid, 2012, págs. 270-272.
[3] VELASCO NÚÑEZ, E., *Delitos cometidos a través de Internet: cuestiones procesales*, ed. La Ley, Madrid, 2010, pág. 200.

comunicaciones y a los datos personales garantizados por la Constitución. Esto es, hasta ahora estas diligencias encontraban el principal obstáculo en su escasa regulación legal, y en su afectación a importantes derechos constitucionalmente protegidos como la intimidad (art. 18), la libertad de expresión (art. 20), el secreto de las comunicaciones (art. 18), la inviolabilidad del domicilio (art. 18) y la protección de datos personales. Pero esto se intenta solucionar a través de esta nueva regulación, que modifica el enunciado del Título VIII Libro II, que pasa a llamarse "De las medidas de investigación limitativas de los derechos reconocidos en el art. 18 de la Constitución", y que regula respectivamente en los Capítulos IV, V, VI, VII, VIII y IX, las siguientes diligencias, la interceptación de las comunicaciones telefónicas y telemáticas; la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen; registro de dispositivos de almacenamiento masivo de información; y registros remotos sobre equipos informáticos. Además, en relación con la protección de datos, establece una orden de conservación y protección de datos por los prestadores de servicios, hasta que se obtenga la autorización judicial para permitir su cesión.

El empleo de estos medios de investigación tecnológicos permiten obtener pruebas de cualquier clase de delito, sea o no un delito informático[4]. Así, resultan eficaces para la investigación de cualquier delito en el que se utilicen dispositivos electrónicos que constituyen una fuente de prueba, debido a la capacidad de almacenamiento de información y a su empleo como medio de comunicación; las pruebas que se obtienen se conocen como pruebas electrónicas[5].

Hay que tener en cuenta igualmente que para la investigación de estos delitos hay que obrar con urgencia, pues los rastros que dejan desaparecen enseguida, por lo que se hace difícil averiguar, si ha pasado mucho tiempo, quién ha sido el autor del delito informático.

En relación a los autores que cometen estos delitos, hay que tener en cuenta que la mayoría son personas jóvenes, y ello se explica por la llamada brecha digital, que se

[4] En este sentido es clave el Convenio sobre Cibercrimen del Consejo de Europa, de 23 de noviembre de 2001, en vigor en España desde el 1 de octubre de 2010, pues las medidas que prevé se aplican no solo a los delitos informáticos que se recogen en él, sino a cualquier delito informático o no-informático en el que existan evidencias digitales.

[5] BUENO DE MATA F., *Prueba electrónica y proceso 2.0*, ed. Tirant lo Blanch, Valencia, 2014, págs. 95-105.

define como la desigualdad que existe entre las personas de distintas comunidades o estados que utilizan las TICs como una parte rutinaria de su vida diaria y aquellas que no tienen acceso a las mismas, o que aunque lo tengan, no saben cómo utilizarlas[6].

Ahora bien, también son autores de estos delitos profesionales cualificados que buscan un beneficio personal y que actúan en el seno de la delincuencia organizada, por lo que se pone de manifiesto que estas acciones tienen una alta carga de trasnacionalidad y una rápida reinvención, obligando a quienes los combaten a tener que actualizarse constantemente. Así, se ha pasado del *hacker* que por motivos de autoestima o rebeldía accedía a sistemas informáticos con alta seguridad y del típico delincuente ocasional que aprovechaba sus conocimientos informáticos para inmiscuirse en intimidades de personajes públicos y para revelar en Internet sus privacidades que no habrían salido a la luz de otra manera, a verdaderos expertos en delincuencia organizada que persiguen un lucro personal[7].

Creemos que presentamos un trabajo muy interesante y con gran interés actual, pues los delitos cometidos a través de Internet tienen una enorme proyección de futuro, y están creciendo con el paso de los años, por lo que es una cuestión de máxima actualidad, al igual que los son las diligencias que se practican para investigarlos. Se trata de un tema reciente y poco tratado a la vez que controvertido, pues su utilización vulnera derechos fundamentales de los sujetos investigados, por lo que en la mayoría de las ocasiones su práctica debe realizarse mediante autorización judicial previa.

2. LAS FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO QUE SE DEDICAN A ESTAS CUESTIONES

Para la investigación de los delitos informáticos y de los delitos cometidos a través de las nuevas tecnologías pero sin ser informáticos, se requiere que los cuerpos policiales que investigan estén especializados, por eso se ha creado dentro de la Policía Nacional y de la Guardia Civil grupos especializados en la investigación de estos delitos.

[6] SERRANO SANTOYO A. y MARTINEZ MARTÍNEZ E., *La Brecha Digital: Mitos y Realidades*, ed. UABC, México, 2003, pág. 175.
[7] VELASCO NUÑEZ, E., *Delitos cometidos…*, op., cit., págs. 44-45.

2.1. BRIGADA DE INVESTIGACIÓN TECNOLÓGICA (BIT)

La Brigada de Investigación Tecnológica se crea como tal en el año 2002, encuadrada en la UDEF, dependiente de la Comisaría General de Policía Judicial, que es el Órgano Directivo de la Dirección General de la Policía encargado de perseguir todo tipo de delincuencia organizada y violenta, económica y fiscal así como el tráfico de drogas y también la delincuencia tecnológica. El origen de la BIT aparece en 1995 al crearse un Grupo de Delitos Informáticos en la BDEF. El Grupo aumenta con la evolución de Internet y se convierte en una sección con cuatro Grupos Operativos. Finalmente en 2002 recibe el nombre actual de Brigada de Investigación Tecnológica[8].

Asimismo cabe hacer mención a la creación en el año 2012 de la UIT que aparece debido al auge de las nuevas tecnologías de la información y las comunicaciones dentro de la Dirección General de la Policía para responder mejor a los nuevos retos de lucha contra el cibercrimen e innovación tecnológica. Esta unidad asume la investigación y persecución de los delitos a través de las tecnologías de la información y comunicación y actúa como Centro de Prevención y Respuesta del E-Crime de la Policía Nacional, y cuenta con dos brigadas, la Brigada de Investigación Tecnológica y la Brigada de Seguridad Informática. Por lo que en la actualidad observamos que la BIT se encuadra dentro de la UIT.

Esta Brigada está destinada a responder a los retos que plantean las nuevas formas de delincuencia, velando por la seguridad de los internautas y de los ciudadanos en general; igualmente, tiene la función de coordinar las operaciones que involucren a diversas Jefaturas Superiores; la formación del personal del Cuerpo Nacional de Policía y otros cuerpos de Policía extranjeros; la representación internacional y la ejecución y/o coordinación de las investigaciones que tengan su origen en otros países[9].

En este punto cabe hacer referencia a la entrevista que le realizaron a Manuel VÁZQUEZ LÓPEZ, Comisario Jefe de la Brigada de Investigación Tecnológica de la Policía[10], en la que dice que la Brigada se estructura en tres secciones. En esta entrevista

[8] "Encuentro con… Manuel Vázquez López, Comisario Jefe de la Brigada de Investigación Tecnológica de la Policía", *Revista Dintel*, nº 28, Madrid, número especial AGE 2008/2009, pág. 34, disponible en el link: http://www.revistadintel.es/Revista1/DocsNum28/Encuentro/Vazquez.pdf.
[9] *BIT – Funciones*, consultado el 15 de Febrero de 2015, disponible en el link: http://www.policia.es/org_central/judicial/udef/bit_alertas.html.
[10] "*Encuentro con…*, op., cit., págs. 34 y 35.

analiza la composición de estas secciones y los concretos delitos que investigan según recogemos a continuación.

La Sección Primera que se compone por dos grupos a su vez:

- Un grupo encargado de investigar los delitos de pornografía infantil, y cuyo objetivo principal es la detección de producción de dicha pornografía en España para proteger y rescatar a los niños que están siendo objeto de abuso, y la detención y puesta a disposición judicial de los responsables. También se realizan operaciones contra la tenencia y distribución de material pornográfico a través de Internet, así como la investigación de los casos de *grooming* y *bulling*.

- Un segundo grupo que investiga los fraudes en las telecomunicaciones y los delitos de calumnias, injurias, amenazas y todos aquellos que se pueden cometer contra la intimidad de las personas, y que se cometan a través de Internet. En esta sección se ha creado el Grupo de Redes Abiertas, para navegar por la red y detectar contenidos ilícitos e iniciar las correspondientes investigaciones si hay indicios de que puede haber materia delictiva y, en su caso, ponerlo en conocimiento de las autoridades correspondientes.

La Sección Segunda está formada por dos grupos igualmente que investigan los fraudes cometidos en Internet (como por ejemplo el *phishing*, el *pharming* o el *malware* bancario):

- Un grupo de seguridad lógica para investigar los delitos de carácter estrictamente informáticos como pueden ser los ataques DDoS, intrusiones, descubrimiento y revelación de secretos, entre otros.

- Un segundo grupo para la investigación de los delitos relativos a la propiedad intelectual e industrial, persiguiendo, principalmente, los fraudes en el uso de las comunicaciones, fraudes en Internet y piratería.

Por último, encontramos la Sección Técnica, que es la encargada de la formación, asimismo se encarga de volcados, análisis forense e I+D.

2.2. GRUPO DE DELITOS TELEMÁTICOS (GDT)

El Grupo de Delitos Telemáticos fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil dependiente de la Comisaría General de Policía

Judicial, los delitos que se cometen a través de Internet[11]. Su origen se encuentra en el año 1996, cuando se constituyó el GDI para atender a las escasas denuncias que había en estos primeros años por estos delitos.

Ahora bien, con el aumento exponencial del uso de Internet se produjo paralelamente un crecimiento de los hechos delictivos que se cometían a través de este medio, por lo que se amplían las competencias del grupo para la investigación, pues se pasa a hablar del cibercrimen, que supone la realización de conductas delictivas a través de los sistemas de información o contra éstos. Y el grupo pasa a llamarse GDT.

Además, en el año 2002 se crean los EDITE,s en cada una de las provincias de España, debido a la gran cantidad de denuncias que se presentaban. La premisa principal para la creación del GDT y de los EDITE,s ha sido, la investigación de la delincuencia que se vale de las redes y sistemas de información para su comisión. También cabe destacar los esfuerzos que realizan para fomentar un uso seguro de las nuevas tecnologías[12], pues ello permitirá reducir el impacto de esta delincuencia, pues si se informa a la ciudadanía sobre ello se logrará un fin preventivo.

El GDT se articula en dos secciones[13]:

- La Sección de Investigación, se estructura en cuatro equipos de investigación que responden a los grupos de delitos que recoge el Convenio sobre Ciberdelincuencia hecho en Budapest el 23 de noviembre de 2001[14].

[11] *La Unidad*, consultado el 15 de febrero de 2015, disponible en el link: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php.
[12] *La Unidad*, consultado el 15 de febrero de 2015, disponible en el link: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php.
[13] SALOMON CLOTET, J., "Delito informático y su investigación", *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, ed. Consejo General del Poder Judicial, Madrid, 2006, pág. 106.
[14] Así, encontramos:
- Un grupo que se encarga de los Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, delitos tales como el acceso ilícito, la interceptación ilícita, interferencia en los datos y en el sistema y abuso de dispositivos; (Capítulo II, Sección I, Título I del Convenio).
- Un segundo grupo que investiga los Delitos propiamente informáticos, como falsificaciones y fraudes informáticas; (Capítulo II, Sección I, Título II del Convenio).
- Un tercer grupo que se encarga de los Delitos relacionados con el contenido, como es el caso de la pornografía infantil; y (Capítulo II, Sección I, Título III del Convenio).
- Un último grupo que investiga los Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (Capítulo II, Sección I, Título IV del Convenio).

- La Sección de Análisis e I+D, que cuenta con colaboradores, tales como entidades públicas, privadas, y expertos hackers capaces de vulnerar la seguridad de los sistemas informáticos ajenos y que no dudan en practicarlo.

Entre las funciones que desarrolla el GDT encontramos la detección de delitos informáticos en Internet y su posterior investigación, la dirección y la formación del personal de los EDITE,s, así como coordinar las actividades de la Guardia Civil en investigaciones internacionales en el ámbito del cibercrimen y promover la participación de la Guardia Civil en foros y encuentros internacionales relacionados con el mismo[15].

Por último cabe destacar la labor conjunta desarrollada por ambos cuerpos especializados, pues, tanto la BIT como el GDT aúnan sus esfuerzos coordinándose y trasladando a la sociedad la implicación de todos los Cuerpos y Fuerzas de Seguridad del Estados en la lucha contra la ciberdelincuencia. Destaca asimismo la labor de colaboración con diferentes fuerzas de seguridad internacionales como INTERPOL o EUROPOL, pues hay que tener en cuenta que en muchas ocasiones los delitos no se cometen en un único país.

2.3. PRINCIPALES DELITOS QUE INVESTIGAN

Los principales delitos que investigan tanto la BIT como el GDT son los delitos que recoge el Convenio sobre Ciberdelincuencia de 1 de Noviembre de 2001 en el Capítulo II, Títulos I, II, III y VI, y son respectivamente:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

Delitos tales como, el descubrimiento y revelación de secretos que se recoge en el art. 197.2 del CP, en casos en los que el delincuente utiliza claves informáticas a las que accede ilegalmente para obtener datos personales recogidos en un fichero con la intención de vulnerar la intimidad de esas personas.

Otro delito de los que se encuadra en este Título es el de interceptación de cualquier tipo de telecomunicaciones, art. 197.1 del CP, como por ejemplo mensajes de correo electrónico, para descubrir secretos que vulneran la intimidad de otros.

[15] SALOMON CLOTET, J., "Delito informático…, op., cit., pág. 106.

- Delitos propiamente informáticos:

Las falsificaciones y fraudes informáticos, en este grupo encontramos por ejemplo el *phishing*, que consiste en suplantar la página web de una entidad de crédito o de cualquier otra empresa de la que se pueda obtener un beneficio económico, haciendo creer al usuario que se encuentra ante la página oficial de esas entidades o empresas[16]. Esto permite a los delincuentes informáticos obtener información personal y las claves de los usuarios para poder realizar transacciones no consentidas por estos. Este tipo de estafa está siendo utilizada habitualmente por grupos del crimen organizado que ven en esta forma de delinquir un enriquecimiento fácil, con menor pena o castigo y menores costes.

Encontramos también delitos como las subastas o ventas a través de Internet que permiten llegar a millones de consumidores, y que presentan el problema de que la única forma de comprobar la existencia del producto es mediante fotografías que pueden falsearse, siendo la víctima de este delito el comprador que puja por un producto que es inexistente, perdiendo todo contacto con el vendedor una vez que realiza el pago. Además, hay que tener en cuenta que la capacidad de conectividad que ofrecen las nuevas tecnologías las convierte en un instrumento muy eficaz en la difusión masiva de engaños y en la ejecución de maniobras defraudatorias.

- Delitos relacionados con el contenido ilícito:

Entre los que encontramos la pornografía infantil, que supone la filmación de imágenes y el tráfico de cualquier material audiovisual que utiliza niños en un contexto sexual a través de Internet. Este delito se castiga en el art. 189 del CP. Encontramos también en este punto el acoso a menores a través de la red, también conocido como *child grooming*, delito tipificado en el art. 183 bis del CP cuando la víctima tiene menor de 13 años, y que cuando es mayor se reconduce a otros tipos penales tales como coacciones, amenazas, delitos contra la integridad moral, descubrimiento y revelación de secretos e incluso pornografía infantil.

[16] FERNÁNDEZ LÁZARO, F., "La Brigada de Investigación Tecnológica: la Investigación policial, *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, ed. Consejo General del Poder Judicial, Madrid, 2006, págs. 134-135.

Entre estos delitos encontramos también el ciberterrorismo, que se define como el ataque premeditado y que se desarrolla por motivos políticos[17], que se lleva a cabo por grupos terroristas, utilizando la tecnología informática para desactivar las infraestructuras electrónicas y físicas de un país, provocando la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, sistemas bancarios, servicio de aeropuertos, o creando virus para corromper las infraestructuras del gobierno de la nación, y provocando así, caos y terror en la población[18]. Un claro caso de ataque ciberterrorista lo tenemos en el ataque sufrido por Estonia en el año 2007.

Por ello, ante la aparición y previsible proliferación de este fenómeno, y debido a la gran alarma social que genera, se crea en el año 2003 la Unidad de Ciberterrorismo en la Guardia Civil, con una estructura similar a la GDT, para apoyar la lucha antiterrorista en todos aquellos aspectos vinculados a las nuevas tecnologías[19].

- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines:

Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática, así como el intercambio de contenidos sometidos a derechos de propiedad intelectual a través de las llamadas redes P2P[20]. Todas estas conductas delictivas encuentran 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".

[17] BUENO DE MATA F., "Ciberterrorismo: tratamiento procesal y penal del terrorismo del futuro", *Estudios actuales en derecho y ciencia política: [2º. Encuentro INCIJUP]*, ed. Andavira, Santiago de Compostela, 2013, pág. 317.
[18] Definición dada por Dan Verton, Periodista especializado en seguridad informática y ex oficial de inteligencia Naval de los Estados Unidos, Washington, D.C. 2003.
[19] BUENO DE MATA F., "Ciberterrorismo…, op., cit., pág. 322.
[20] GÓMEZ TOMILLO M., "Responsabilidad penal por delitos contra la propiedad intelectual cometidos a través de Internet", *La propiedad intelectual en la era digital. Límites e infracciones a los derechos de autor en Internet*, ed. La Ley, Madrid, 2011, pág. 212.

2.4. PROTOCOLOS DE ACTUACIÓN[21]

Cabe sistematizar la investigación de los delitos cometidos utilizando las nuevas tecnologías en tres fases:

- Fase previa:

Esta fase va a permitir acreditar la existencia de un delito. Se inicia con el conocimiento del delito, bien a través de denuncia si estamos ante un delito privado o por la simple comunicación del hecho en el caso de que estemos ante un delito público. Asimismo cabe hacer referencia a la posibilidad que se ofrece en la Página Web de la Policía de presentar una denuncia electrónica, así como la posibilidad de usar las vías telemáticas para informar de una presunta actividad delictiva. Esto hay que encuadrarlo en el Plan Estratégico para la Modernización de la Administración de Justicia y en el Plan de Acción de la Secretaría General de la Administración de Justicia, para la consolidación de la modernización tecnológica[22].

En esta fase la actuación que hay que llevar a cabo comprende la inspección ocular del lugar o lugares en los que haya podido pasar la comunicación delictiva, y hay que aislar el ordenador con el que se ha llevado a cabo el delito, en busca de indicios que permitan entender lo que ha sucedido y que permita iniciar la investigación. Ahora bien, hay que tener en cuenta que el hecho de aislar el equipo informático puede afectar a la intimidad de la víctima ya que supone ver la totalidad del equipo en el que puede guardar información personal. Por ello, el Tribunal Constitucional, en la STC 173/2011, de 7 de noviembre, considera necesario 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 informática así como de las nuevas tecnologías de la información, y dispone 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

[21] Instrucción nº 1/2008 sobre la dirección por el Ministerio Fiscal de las actuaciones de la Policía Judicial, Capítulo VI: Las distintas fases de actuación de la Policía Judicial, págs. 18-22.
[22] BUJOSA VADELL L.M., "Introducción", *FODERTICS II: hacia una justicia 2.0. Estudios sobre derecho y nuevas tecnologías*, ed. Ratio Legis, Salamanca, D.L. 2014, págs. 12-15.

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[23].

- Fase de investigación:

Esta fase consiste en identificar las conexiones vinculadas con el delito y resolver los datos de tráfico para ubicar el equipo informático e identificar al abonado titular de la conexión, y una vez localizado el equipo e identificado el abonado, se intentará identificar al usuario del ordenador. Para ello sirve de punto de partida los datos del abonado de la conexión a Internet y es fundamental la labor operativa del grupo investigador, que debe tener en cuenta los hábitos de los internautas, en relación a la repetición de lugares de conexión.

Si bien, hay que tener presente, que para la investigación de los delitos cometidos utilizando las nuevas tecnologías, se requieren conocimientos sobre el funcionamiento de Internet, teniendo en cuenta que se articula como una red. Así, cuando te conectas a Internet se establece una comunicación del equipo con el proveedor de acceso a Internet que te asigna un número IP que permite identificarte, este número es único. Para que ordenadores distintos se entiendan se han diseñado unos protocolos de comunicación que se han de respetar[24], estos consisten en paquetes de información que contienen las IP,s de origen y destino, estos datos se conocen como datos de tráfico[25]. Así, para investigar una comunicación delictiva hay que investigar esos datos de tráfico que nos permitirá conocer el ordenador origen de la comunicación. Una vez que tenemos el número IP y conocemos el momento concreto en el que se ha producido la conexión podemos identificar el ordenador, su ubicación y el abonado de la conexión telefónica o del contrato de acceso a Internet.

Ahora bien, hay que poner de manifiesto que las IP,s señalan el concreto equipo informático utilizado para cometer el delito por el presunto delincuente, pero no aportan nada sobre el usuario, y este podría ser el abonado, un familiar, un usuario habitual, uno

[23] 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, Madrid, D.L. 2013, pág. 48.
[24] SALOM CLOTET J., "Delito informático…, op., cit., pág. 109.
[25] En este sentido el Convenio sobre la Ciberdelincuencia establece que por «datos sobre el tráfico» se entenderá cualesquiera datos informáticos relativos a 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.

accidental o incluso uno remoto al equipo. Por lo que posteriormente hay que investigar los datos de tráfico para localizar el origen de la comunicación y así ubicar el equipo informático y vincularlo a un usuario persona física como autor material de los hechos. En este punto cabe hacer referencia a los *logs*, que es un registro de los sucesos que ocurren en el sistema y que se guarda en los servidores, en él se almacenan los eventos del sistema incluidos los datos de tráfico, por ello será uno de los principales elementos de investigación, al contener los datos que se buscan[26].

Para la obtención de estos "datos de tráfico" el Tribunal Supremo ha legitimado la utilización de diversos medios, debido a que no existe una regulación de los mismos por parte del legislador. Así las cosas, el TS ha consentido la utilización de un scanner para la captación policial de los códigos IMSI e IMEI correspondientes a los terminales de telefonía móvil[27], el empleo de software para la obtención de la dirección IP mediante rastreos policiales en Internet de datos procedentes de programas P2P[28], y el uso de balizas de seguimiento GPS para la localización de embarcaciones en alta mar[29]; pues la utilización por la policía de estos medios para la localización geográfica de determinados dispositivos electrónicos no vulnera el derecho fundamental al secreto de las comunicaciones ni supone una injerencia excesiva sobre el derecho fundamental a la intimidad, a los efectos de exigir un control jurisdiccional previo[30].

Según el TS la utilización policial de estos novedosos instrumentos electrónicos en labores de investigación criminal ha sido admitida porque se trata de diligencias de investigación legítimas al no interferir en ningún derecho fundamental que requiera la previa autorización judicial, como por ejemplo en el caso del empleo de balizas de GPS; o bien porque lo que hace la policía es obtener una información que el propio usuario de la red es quien la ha introducido, en el caso del rastreo de direcciones IP; o bien lleva a cabo labores de vigilancia, en el caso de captura de los códigos IMSI/IMEI[31].

En este punto cabe asimismo señalar que también ha legitimado reiteradamente el propio TS uno de los avances tecnológicos más utilizado en la lucha contra el crimen, nos referimos al sistema informático SITEL de interceptación de las

[26] SALOM CLOTET J., "Delito…, op., cit., pág. 110.
[27] STS de 28 de enero de 2009.
[28] STS de 28 de mayo de 2008.
[29] STS de 19 de diciembre de 2008.
[30] ORTIZ PRADILLO J.C., "La investigación…, op., cit., pág. 25.
[31] ORTIZ PRADILLO J.C., "La investigación…, op., cit., pág. 25.

telecomunicaciones, que sustituye a las convencionales grabaciones en cintas magnetofónicas. Este sistema además de que permite la escucha de conversaciones telefónicas del terminal intervenido, aporta también datos relacionados con la localización de ese terminal cuando se realiza la comunicación. Ahora bien, hay que tener en cuenta que este sistema de intervención de las comunicaciones afecta al derecho al secreto de las comunicaciones del art. 18.3 de la CE.

Hasta ahora no existía una regulación legal de este sistema, pues la regulación que la LECrim hacía de la intervención de comunicaciones postales en los arts. 579 a 588 se quedaba corta[32]. Por ello, ha sido el TS el que ha analizado en varias sentencias el rango jurídico de la regulación de los requisitos técnicos y operacionales para proceder a ejecutar los mandamientos judiciales de interceptación de las comunicaciones[33], el funcionamiento de los servidores centrales y los niveles de seguridad en cuanto al acceso a la información allí alojada y su grabación en un DVD que debe ser sellado digitalmente para su posterior entrega a la autoridad judicial[34], el bloqueo de los datos contenidos en el servidor central una vez que concluye la investigación que motivó la interceptación y el régimen de su posterior borrado físico a instancias de la autoridad judicial[35]. Todo ello le ha permitido llegar a la conclusión, en varias sentencias, entre otras, la STS de 19 de julio de 2010, que SITEL cumple con todas las exigencias y garantías propias que se exigen a las diligencias de investigación que cuentan para su práctica con una autorización judicial previa, por lo que como hemos señalado al principio, ha legitimado su uso[36].

Pero hay que advertir que en el Proyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, presentado por el Consejo de Ministros el 13 de Marzo de 2015, prevé un Capítulo, el V, especialmente dedicado a la interceptación de las comunicaciones telefónicas y telemáticas, se pretende recoger esa jurisprudencia dictada por el TS que legitima su uso, y establecer así, la regulación legal de esta diligencia.

---

[32] PÉREZ GAIPO J., "Intervención de las comunicaciones, nuevas tecnologías y derechos procesales: viejos principios para nuevas realidades", *FODERTICS II: hacia una justicia 2.0*, ed. Ratio Legis, Salamanca, 2014, págs. 124 y 125.
[33] STS, Sala 3ª de 5 de febrero de 2008.
[34] STS de 5 de noviembre de 2009.
[35] STS de 6 de junio de 2011.
[36] ORTIZ PRADILLO J.C., "La investigación…, op., cit., pág. 26.

- Fase incriminatoria:

Esta fase comprende la intervención de los equipos informáticos, su análisis, la redacción del correspondiente informe incriminatorio y la puesta a disposición judicial del usuario autor del delito.

La intervención de los equipos se lleva a cabo mediante la práctica de un registro domiciliario, que requiere la obtención de una autorización judicial previa, y que tiene como finalidad la intervención material de los dispositivos informáticos susceptibles de contener indicios de criminalidad.

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 extracción del disco duro y a su clonación forense, siempre en presencia de los usuarios del equipo, que supone hacer una réplica exacta del disco duro en otro vacío[37].

Mientras se realiza la clonación, 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[38].

Se debe igualmente anotar la marca, modelo y número de serie de los discos duros. Procediendo posteriormente al etiquetado de los dispositivos y la entrega de los mismos al Notario, para que los custodie, pues es el Notario el que da fe y garantiza la no manipulación durante todo el proceso, esto es, garantiza la cadena de custodia. Para ello se suelen desplazar los equipos a la notaría, en presencia de los implicados y

[37] ALDAMA SAÍNZ C., "Vulnerabilidades en periciales informáticas", *FODERTICS II: hacia una justicia 2.0. Estudios sobre derecho y nuevas tecnologías*, ed. Ratio Legis, Salamanca, D.L. 2014, pág. 21.

[38] *El proceso de clonación*, consultado el 3 de marzo de 2015, disponible en el link: http://www.ondataforensic.com/proceso-de-clonacion.php.

testigos, para que se facilite la tarea al Notario, pues hay que tener en cuenta que se trata de procesos largos. Además, teniendo en cuenta la posibilidad de manipulación de los dispositivos de almacenamiento de información, es muy importante que todo el proceso esté documentado desde el inicio y se levante acta por parte del perito[39].

Una vez que tenemos la copia se inicia el proceso de análisis que persigue la localización, identificación y aseguramiento de cuantas evidencias se hallen para construir la prueba de indicios, y que permitan vincular al equipo informático con el usuario y con los indicios, permite por tanto vincular un usuario concreto al hecho delictivo que se ha cometido y determinar su responsabilidad criminal[40].

En cuanto a los protocolos de actuación que se desarrollan, cabe hacer mención a la Estrategia de Ciberseguridad Nacional[41], promovida por el Consejo de Seguridad Nacional, en la que se fijan las directrices generales del uso seguro del ciberespacio, mediante la coordinación y cooperación de todas las Administraciones Públicas entre ellas, con el sector privado y con los ciudadanos. Esta estrategia tiene como objetivo lograr un uso seguro de los Sistemas de Información y Telecomunicaciones, a través de la prevención, defensa, detección y respuesta a los ciberataques.

3. PRINCIPALES DILIGENCIAS DE INVESTIGACIÓN

En este punto hablaremos de las principales diligencias de investigación tecnológicas con las que cuenta la Policía Judicial para investigar cualquier delito que se cometa utilizando las nuevas tecnologías y para identificar a su presunto autor. Algunas de ellas, las más importantes, son:

3.1. ADN

La prueba del ADN es una prueba científica que cuenta con una fiabilidad casi absoluta[42], pues las características del ADN son únicas en cada persona, y se puede obtener a través de restos biológicos como saliva, sangre, semen o cabello que deja el

[39] ALDAMA SAÍNZ C., "Vulnerabilidades…, op., cit., págs. 22 y 23.
[40] SALOM CLOTET J., "Delito informático…, op., cit., págs. 111-120.
[41] *La Estrategia de Ciberseguridad Nacional*, 2013, consultada el 11 de abril de 2015, disponible en el link: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf
[42] CABEZUDO BAJO M.J., "La regulación del "uso forense de la tecnología del ADN" en España y en la UE", *FODERTICS, estudios sobre derecho y nuevas tecnologías*, ed. Andavira, Santiago de Compostela, 2012, pág. 103.

autor en la escena del crimen o en la propia víctima[43]. Estos restos biológicos permiten situar al presunto delincuente en el lugar donde se ha cometido el delito y atribuirle su autoría si se da una relación de causalidad, esto es, si se pueden conectar esos restos con la realización de la conducta desaprobada socialmente.

La práctica de esta diligencia se prevé en el art. 363.2 de la LECrim., al decir que "siempre que concurran acreditadas razones que lo justifiquen, el Juez de Instrucción podrá acordar, en resolución motivada, la obtención de muestras biológicas del sospechoso que resulten indispensables para la determinación de su perfil de ADN".

Ahora bien, hay que hacer referencia a los problemas que presenta esta diligencia, pues hay que recordar que la prueba de ADN tiene que ser obtenida de la forma más fiable posible lo que supone que debe asegurarse la integridad de la muestra, y tiene que ser obtenida lícitamente, esto es, respetando los derechos fundamentales. Esta diligencia presenta 3 fases fundamentales[44]:

- Obtención de la muestra de ADN, recogiéndola de la escena del crimen[45] o del cuerpo de la víctima, se trata por tanto de una muestra no identificada. Posteriormente hay que recoger una muestra corporal de una persona identificada[46] para así obtener una muestra indubitada para tomar de referencia.

- Extracción del perfil de ADN, con las muestras obtenidas en la fase anterior se elabora el perfil de ADN del sospechoso y se compara con el obtenido en el lugar del crimen.

- Tratamiento del dato de ADN en la base de datos, la obtención de muestras biológicas tiene como destino el banco policial de perfiles de ADN, no

[43] DEL POZO PÉREZ M., "Algunas cuestiones polémicas sobre el ADN y el proceso penal", *Revista general de derecho público comparado*, Nº 10, 2012.
[44] CABEZUDO BAJO M.J., "La regulación…, op., cit., pág. 107.
[45] En este sentido el art. 326 párrafo 3º de la LECrim dice que cuando se pusiera de manifiesto la existencia de huellas o vestigios cuyo análisis biológico pudiera contribuir al esclarecimiento del hecho investigado, el Juez de Instrucción adoptará u ordenará a la Policía Judicial o al médico forense que adopte las medidas necesarias para que la recogida, custodia y examen de aquellas muestras se verifique en condiciones que garanticen su autenticidad.
[46] En este sentido el art. 363 párrafo 2º de la LECrim señala que siempre que concurran acreditadas razones que lo justifiquen, el Juez de Instrucción podrá acordar, en resolución motivada, la obtención de muestras biológicas del sospechoso que resulten indispensables para la determinación de su perfil de ADN. A tal fin, podrá decidir la práctica de aquellos actos de inspección, reconocimiento o intervención corporal que resulten adecuados a los principios de proporcionalidad y razonabilidad.

con fines de identificación, sino para su inclusión a efectos de investigación criminal, sobre hechos pasados, presentes o futuros[47].

Esta diligencia presenta varios problemas, el primero, en relación a si puede ser recogida sin la correspondiente autorización judicial una muestra abandonada por el sospechoso cuando se conocía su identidad, esto ha sido resuelto por Acuerdo del Pleno no jurisdiccional de la Sala Segunda del TS de 31 de enero de 2006, en la que se establece que se puede proceder a la recogida por parte de la Policía Judicial de estas muestras biológicas abandonadas por el sospechoso sin necesidad de la previa autorización judicial.

Ahora bien, el punto más conflictivo de esta diligencia, hasta ahora, era que se necesita el consentimiento del afectado, y en su defecto una resolución judicial suficientemente motivada, para poder obtener las muestras biológicas de una persona sospechosa identificada. Pero teniendo en cuenta que, si el sospechoso está detenido el consentimiento se habría de prestar en presencia de su abogado, siendo informado de modo claro y concluyente de que la pericia podría incriminarle.

Es en este punto donde aparecen los mayores problemas, pues hasta el año 2010 no era necesario para obtener una muestra de ADN a los detenidos, a través de un frotis bucal, que estos estuvieran asistidos de abogado, pero la STS de 30 de julio de 2010 cambió la práctica, al entender que es una garantía jurídica necesaria el asesoramiento de los detenidos por parte de los abogados. Asimismo, hay que tener presente que si no consienten, para tomar muestras de ADN será indispensable una autorización judicial, pero teniendo en cuenta que solo podrá hacerse efectiva cuando no se violente al acusado. Esto ha sido ratificado por Acuerdo de la Sala de lo Penal del TS, de 24 de septiembre de 2014, en el que establecía que, al amparo de la defensa del derecho a la intimidad, "la toma biológica de muestras para la práctica de la prueba de ADN con el consentimiento del imputado necesita la asistencia del letrado cuando el imputado se encuentra detenido, o, en su defecto, autorización judicial".

Todo esto ha provocado que desde el año 2011 se haya reducido drásticamente las bases de datos de ADN, lo que supone un gran inconveniente, pues los abogados se acogen en este derecho a la intimidad de los acusados para no facilitar la muestra, y hay

[47] En este sentido se aprobó la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

que tener en cuenta que aunque medie autorización judicial, si el detenido se niega no pude extraérsele la muestra, por lo que se está produciendo un vaciamiento de las bases de datos de ADN, lo que va a afectar en la resolución de los casos. Este vaciamiento de las bases de datos de ADN se podría solucionar si se obtuvieran al nacer las muestras y se incorporaran a bases de datos seguras.

El problema de la oposición por parte del detenido a la toma de la muestra se pretende solucionar con el Proyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, presentado por el Consejo de Ministros el 13 de Marzo de 2015, en el que se establece expresamente que "si el detenido se opusiera a la recogida de las muestras mediante frotis bucal, conforme a las previsiones de la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir de ADN, el juez de instrucción, a instancia de la Policía Judicial o del Ministerio Fiscal podrá imponer la ejecución forzosa de tal diligencia mediante el recurso a las medidas coactivas mínimas indispensables, que deberán ser proporcionadas a las circunstancias del caso y respetuosas con su dignidad".

Se pretende instaurar en caso de oposición su ejecución forzosa, y creemos que hay que encuadrar esta nueva regulación en el hecho de que se trata de una diligencia muy fiable, y que presenta numerosas ventajas, pues además de que permite resolver muchos casos, es también una de las principales causas de exculpación de condenados por error, un claro ejemplo es el Caso Wanninkhof, donde fue la prueba del ADN obtenida de un cigarrillo encontrado junto al cadáver, la que sirvió para localizar años más tarde y tras un segundo asesinato al verdadero culpable, y exculpar a la condenada erróneamente.

Así, se pone de manifiesto que, aunque las muestras de ADN que se recojan de las escenas del crimen queden sin identificar, si posteriormente se detiene a una persona y se le extrae el ADN y coincide, se pueden resolver los crímenes anteriores en los que hubiera participado y en los que estuviera implicado.

Por último, cabe poner de manifiesto que el mayor inconveniente que presenta esta diligencia es que no tiene una regulación de los protocolos de actuación que ha de seguir la Policía Científica en la recogida de muestras de ADN, y habrían de regularse

en todo caso para asegurar la integridad y fiabilidad de la muestra, ello a fin de evitar la contaminación de la muestra por el propio personal que la recoge, o por su alteración en el traslado. En este sentido hay que tener en cuenta los estudios desarrollados por la ISFG en la que se establecen los requisitos que debe cumplir el personal que recoge las muestras, las precauciones que deben tomar en la recogida de las muestras, en su posterior envío al laboratorio, cómo ha de documentarse la recogida, que condiciones deben cumplirse en la toma de muestras indubitadas, así como en la recogida de muestras biológicas de la escena del crimen, y como han de preservarse esas muestras[48].

3.2. BIOMETRÍA

Cuando en la investigación de un delito no se cuentan con restos biológicos que permitan identificar al autor de un delito a través de la prueba del ADN, hay que acudir a la biometría, que es una técnica consistente en el uso de las tecnologías para analizar las características corporales o el comportamiento del presunto delincuente y que son utilizadas por profesionales de los Cuerpos y Fuerzas de Seguridad del Estado, concretamente por la sección de Antropología Forense.

Se distinguen dos grupos de registros biométricos[49]:

- Los que analizan rasgos corporales o morfológicos, esto es, analizan las características físicas inalterables y presentes en todas las personas como por ejemplo el iris o la huella dactilar.

- Los que analizan el comportamiento, la conducta de las personas, como por ejemplo las pulsaciones del teclado o la firma. En este último caso a través de una pericial caligráfica se puede llegar a atribuir dicha firma a su autor y determinar las condiciones bajo las que la realizó, esto es, si por ejemplo fue coaccionado para firmar.

Se ha potenciado con la aparición de las nuevas tecnologías la identificación de individuos a partir de rasgos biométricos, y en la actualidad se están desarrollando diligencias como el reconocimiento de iris, de huellas dactilares, de voz o de caras. Pero todavía quedan lejos otras técnicas de identificación, como por ejemplo la termografía

[48] CABEZUDO BAJO M.J., "La regulación…, op., cit., págs. 109-110.
[49] BUENO DE MATA, F., "Nuevas tecnologías y diligencias", *FODERTICS, estudios sobre derecho y nuevas tecnologías*, ed. Andavira, Santiago de Compostela, 2012, págs. 91-101.

facial basada en cámaras infrarrojas que detectan patrones de calor creados por el flujo sanguíneo emitido por la piel.

Así, las técnicas que se utilizan para identificar a presuntos delincuentes a falta de restos biológicos y huellas dactilares son los retratos robots y los reconocimientos faciales, siempre que se disponga de una imagen o del testimonio de testigos capaces de describirlos y recordarlos[50].

En cuanto a los retratos robot, hay que decir que su utilización es residual, cuando se han agotado las vías de investigación o cuando no hay ningún otro tipo de pista. Se realiza el retrato a través de programas informáticos como *Faces 3.0*, que contiene una lista con los rasgos faciales más relevantes. Se suele utilizar en casos en los que hay al menos un testigo ocular, si bien hay que tener presente que no goza de una gran fiabilidad pues los recuerdos de los testigos oculares pueden no ser lo suficientemente claros y precisos, o no se plasman bien por los agentes, por lo que sería más conveniente que fueran los propios testigos los que elaboraran el retrato. Por lo que todavía faltan avances en estos programas de creación de retratos[51].

En cuanto a los reconocimientos faciales, hay que partir de que los rasgos faciales de cada persona son propios, y hay que tener en cuenta que esta forma de reconocimiento ha avanzado debido al aumento de la presencia de cámaras de vídeo tanto en lugares de trabajo, como en calles, establecimientos y hogares. Esta identificación es llevada a cabo por profesionales con gran experiencia a través de la localización de una cara en una foto o secuencia de vídeo y compararla con una imagen de la que se dispone en una base de datos, lo que supone que exista una base de datos lo suficientemente amplia, que no existe hasta el momento. Esta comparación permite verificar o descartar si estamos ante la misma persona basándonos en los elementos estructurales de su cara[52]. Ahora bien, tenemos que decir que todavía hacen falta muchos avances en biometría en lo que a reconocimientos faciales se refiere, pues por ejemplo no permiten los programas hasta ahora desarrollados llevar a cabo un reconocimiento del rostro si se llevan en él objetos como gafas o barba.

Otras técnicas biométricas que se están aplicando en España son por ejemplo el reconocimiento mediante el iris del ojo, que supone un escaneo digital del iris mediante

[50] BUENO DE MATA, F., "Nuevas tecnologías…, op., cit., pág. 95.
[51] BUENO DE MATA, F., "Nuevas tecnologías…, op., cit., pág. 96.
[52] BUENO DE MATA, F., "Nuevas tecnologías…, op., cit., págs. 97-99.

fotografías, y cabe mencionar como inconveniente de este tipo de reconocimiento que se trata de una práctica muy intrusiva. También cabe el reconocimiento a través del pabellón auricular, que se basa en la forma de la oreja, en la estructura del cartílago, y que supondría una identificación similar a la que se realiza mediante la huella dactilar.

Asimismo hay otros tipos de reconocimiento que todavía no se han desarrollado en nuestro país debido al alto coste que suponen, como el reconocimiento mediante las venas de la mano, que consistiría en capturar imágenes del patrón del flujo sanguíneo de la mano; o la termografía facial, que consiste en cámaras infrarrojas que detectan patrones de calor creados por el flujo sanguíneo en la cara.

Por último encontramos otros tipos de reconocimiento biométricos que requieren todavía de una mayor investigación y desarrollo, como es el caso del reconocimiento por sensor de olor que capturaría los compuestos químicos que emiten los poros de la piel; o el reconocimiento de movimiento, que supone capturar una secuencia de imágenes que permitan analizar el característico movimiento de cada persona[53].

En este punto cabe señalar que esta diligencia cobra importancia, y entra en funcionamiento, cuando ante la comisión de un delito, no se cuenta con escenario del crimen, y además tampoco se encuentran huellas dactilares, por lo que en principio no podríamos identificar al autor, y es en estas situaciones cuando la Policía debe hacer uso de estas técnicas biométricas. Asimismo hay que recurrir a esta diligencia en los casos en los que los delincuentes recurren al disfraz o a la cirugía para no ser reconocidos al cometer un hecho delictivo[54].

La crítica que cabe hacer a esta diligencia es que precisa de un mayor desarrollo, lo que lleva implícito a su vez una mayor inversión en estas nuevas técnicas de identificación, creando unos programas informáticos que permitan obtener unos resultados fiables, y que se pongan a disposición de los cuerpos policiales que investigan, pues como hemos señalado antes, creemos que es muy eficaz para identificar a los delincuentes en los casos en los que no se encuentra ni ADN, ni huellas dactilares en el lugar del crimen.

Por último, señalar que con los avances que han supuesto las TICs, podría producirse una autentificación biométrica más fiable, esto nos permitiría hablar de la

[53] BUENO DE MATA, F., "Nuevas Tecnologías…, op., cit., págs. 99-100.
[54] BUENO DE MATA, F., "Nuevas Tecnologías…, op., cit., págs. 91 y 100.

biometría informática, que consistiría en la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos y conductuales para identificar a un individuo[55].

3.3. ENTREGAS VIGILADAS A TRAVÉS DE INTERNET

Esta concreta diligencia de investigación se prevé para el terreno físico en el art. 263 bis de la LECrim y consiste en la posibilidad de que el objeto delictivo circule o sea entregado vigiladamente incluso por agentes de las Fuerzas y Cuerpos de Seguridad del Estado, con la idea de que en los delitos cometidos por grupos organizados puedan aflorar, y ser así descubiertos los máximos partícipes posibles implicados en la cadena delictiva, tanto dentro como fuera de España, y especialmente, los superiores jerárquicos, que suelen ser los que hacen la transmisión mediata del objeto del delito[56]. De ello se deduce que está especialmente prevista para investigar casos de delincuencia organizada que se dedica al tráfico de drogas o de armas o al blanqueo de capitales.

Hay que mencionar asimismo que esta medida puede ser utilizada igualmente para perseguir la delincuencia organizada informática, en casos de terrorismo o pornografía infantil, por ejemplo. Si bien hay que decir que esta diligencia presenta un problema o dificultad en el caso en el que nos encontremos ante un delito informático, y es el siguiente, que los cuerpos policiales, a diferencia de lo que ocurre en el terreno físico, no pueden asegurar el debido control de lo que circula a través de las telecomunicaciones que se hacen por la Red[57]; así, por ejemplo, en este punto cabría preguntarse ¿cómo controlamos un archivo con contenido sexual de un menor de edad que circula por la red?

Por ello, la utilización de esta técnica para la investigación de los delitos informáticos supondría su acompañamiento con fórmulas técnicas de control, que son las garantías a las que se refiere el art. 263 bis relativo a la entrega vigilada en el terreno físico, garantías concretas que han de respetarse a la hora de practicar esta diligencia en cualquier ámbito, ya sea el físico o el informático, y que son:

- Un acuerdo judicial fundado ya que pueden verse afectados o restringidos derechos fundamentales del investigado, en el que se determine

[55] BUENO DE MATA, F., "Nuevas Tecnologías…, op., cit., pág. 93.
[56] VELASCO NUÑEZ, E., *Delitos cometidos…,* op., cit., págs. 202-203.
[57] VELASCO NUÑEZ, E., *Delitos cometidos*…, op., cit., págs. 204-205.

explícitamente si es posible el objeto de autorización o entrega cuya circulación se tolera, indicando el tipo y cantidad de la sustancia de que se trate.

- Hay que tener en cuenta para su adopción la necesidad a los fines de la investigación ponderando la importancia del delito, las posibilidades de la vigilancia y la posible afección colateral de otros intereses dignos también de protección.

- El recurso a la entrega vigilada se hará caso por caso y, en el plano internacional, se adecuará a lo dispuesto en los tratados internacionales.

- Se requiere en relación a la interceptación y apertura de ficheros o archivos sospechosos de la actividad delictiva investigada, y en su caso la posterior sustitución de lo aprehendido con el objeto de descubrir la autoría de aquel a quien se le dirigía, la intervención judicial por afectar al secreto en las telecomunicaciones, por lo que se requiere la previa autorización por el Juez de Instrucción[58].

En relación a la utilidad de esta diligencia, hay que decir que en el ámbito de la delincuencia organizada informática sería muy útil, por ejemplo en casos de ciberterrorismo, fraudes y pornografía infantil, permitiendo que el objeto delictivo, teniendo en cuenta que en este caso son ficheros informáticos, circulen teniéndolos vigilados por agentes especializados, para así poder descubrir al máximo número de partícipes implicados.

Si bien hay que apuntar en último lugar que hasta ahora no existe una regulación legal específica en materia de entrega vigilada a través de Internet, pero hay que tener en cuenta, siguiendo la exposición hecha, que sería sencilla la regulación, pues solo haría falta eliminar la concreta mención que hace el art. 263 bis a las drogas tóxicas, estupefacientes o sustancias psicotrópicas, por otra más genérica que abarcara a todos estos nuevos delitos tecnológicos.

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

3.4. TECNOVIGILANCIA, BALIZAS Y GPS

La tecnovigilancia, es una especie de espionaje técnico, y supone el sometimiento a control mediante dispositivos técnicos de las actividades y movimientos de una persona, teniendo en cuenta que abarca todo tipo de control telemático de sus actividades, pero considerando igualmente que solo la información relacionada con la actividad delictiva que se está investigando será relevante, pues lo que se pretende con esta diligencia es probar que se ha realizado una actividad delictiva pasada, como por ejemplo al observar quién accede a un objeto robado, actual o futura, al observar por ejemplo las actividades de sospechosos de un delito para ver si lo reiteran.

Se trata por tanto de realizar una vigilancia sin apenas contacto físico a través de máquinas que reciben y emiten imagen y sonido, y la envían a centrales de vigilancia donde se ven y escuchan, estas imágenes y sonidos sirven como apoyo y complemento del testimonio del vigilante, lo que le aporta a este testimonio una mayor credibilidad[59].

No hay que perder de vista en todo caso que el uso de esta vigilancia técnica plantea dos problemas fundamentales, que son, por un lado, la afectación a terceras personas que son en todo caso ajenas al delito que se ha cometido, y cuyas intimidades o incluso actuaciones delictivas se hacen públicas sin necesidad; y, por otro lado, hay que tener presente que si bien es cierto que captan situaciones objetivas en las que no cabe introducir apreciaciones subjetivas, plantea problemas relacionados con la contextualidad, en el sentido de que puede ser una emisión sesgada y sacada de contexto, la no manipulación y el destino que se dará a la prueba, una vez usada, para no afectar otros bienes jurídicos protegibles[60]. Estas son las desventajas que presenta esta diligencia. Asimismo otro punto cuestionable de esta diligencia es que permite un conocimiento preciso de la vida privada del individuo, lo que puede suponer riesgos para los derechos y libertades de las personas vigiladas.

Si bien hay que apuntar igualmente que estos problemas que presenta esta diligencia se podrían solucionar y evitar si existiera una regulación legal con garantías que sometiera en todo caso el uso de esta diligencia a control judicial.

---

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

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

Encontramos también otros medios de investigación que son los dispositivos de control remoto, que incluyen tanto balizas como GPS:

- Las balizas son dispositivos electrónicos sofisticados que a través de técnicas de emisión y recepción de señales de localización, sitúan objetos, tales como vehículos o embarcaciones en una ubicación geográfica muy aproximada, y con ello permiten el control de los mismos y de quienes los utilizan[61].

- El sistema GPS recoge la señal emitida desde un dispositivo electrónico y determina su localización al paso de uno de los muchos satélites GPS en órbita de la tierra sobre el dispositivo emisor, permitiendo la localización y seguimiento en tiempo real de los objetivos, y facilita su control[62].

En este punto conviene tener en cuenta que se trata de diligencias o medios técnicos de geolocalización, ya que solo permiten conocer la ubicación de las personas, por lo que no afectan a los derechos fundamentales de los presuntos delincuentes que están siendo investigados, o lo hacen en todo caso con una menor incidencia, pues son mucho menos intrusivas.

En ese sentido, el propio TS en una sentencia de 22 de junio de 2007 en la que se cuestionaba la posible vulneración del derecho a la intimidad por la colocación policial de una baliza en una embarcación dedicada al tráfico de drogas pata facilitar su seguimiento en alta mar, establece que "no se precisó ninguna injerencia en ámbitos de intimidad constitucionalmente protegidos"... ya que "se trata, de una diligencia de investigación, legítima desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiriera en un derecho fundamental que requeriría la intervención judicial".

Sin embargo, una sentencia posterior del propio TS, de 19 de diciembre de 2008, en relación con el sistema de GPS, establece un matiz, al señalar que se podría ver vulnerado el derecho a la intimidad de la persona a la que se geolocaliza, si con ello podemos conocer el lugar en el que se encuentra el investigado de forma exacta y en

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

[62] LLAMAS FERNÁNDEZ M. y GORDILLO LUQUE J.M., "Medios técnicos de vigilancia", *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, ed. Consejo General del Poder Judicial, Madrid, D.L. 2007, págs. 229 y 230.

todo momento, y en estos casos se precisaría en todo caso para el desarrollo de esta diligencia una autorización judicial previa. Ahora bien, si por el contrario, este sistema no te permite conocer la ubicación con exactitud, sino que solo aproximadamente, teniendo en cuenta la estación repetidora que capta la señal, en estos casos en modo alguno puede considerarse afectado, de forma relevante, el derecho a la intimidad del sometido a la práctica de la diligencia.

Estos problemas que surgían al acordar la práctica de estas medidas se pretenden solventar con el Proyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, presentado por el Consejo de Ministros el 13 de Marzo de 2015, que regula en el art. 588 quinquies b, la utilización de estos dispositivos o medios técnicos de seguimiento y localización, que dice que "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". Asimismo se prevé para evitar la vulneración de derechos fundamentales un límite temporal máximo de 2 años, y que la información obtenida sea debidamente custodiada para evitar su utilización indebida

Cabe concluir señalando que estamos ante tres diligencia muy útiles para llevar a cabo un acercamiento al presunto delincuente que nos permita confirmar si es el autor o no del hecho delictivo, y los medios tecnológicos son muy adecuados para ello, teniendo siempre en cuenta que un uso abusivo y sin control supone una intrusión y vulneración de derechos fundamentales, y en este punto había que tener especial cuidado al no existir, hasta ahora, una regulación legal.

3.5. AGENTE ENCUBIERTO EN INTERNET

Esta diligencia consiste en infiltrar en la red a un agente de las Fuerzas y Cuerpos de Seguridad del Estado especializado[63], para que, actuando desde la clandestinidad y ocultando su verdadera identidad, aunque siempre con sujeción a la ley, arrastre y saque a la luz a los autores de delitos informáticos, y para ello se necesita forjar una relación de confianza con el delincuente que permita al agente integrarse durante un largo periodo de tiempo en el ambiente o mundo que rodea a esos ciberdelincuentes, para

[63] Este agente encubierto en Internet debe tener conocimientos informáticos, por ello, se utilizan agentes de la BIT o de la GDT.

obtener la información que permita desenmascararlos[64], información para conocer las actividades ilícitas de la banda organizada, la identidad de sus miembro o las relaciones con otros entes similares, esto es, todos los datos posibles acerca del grupo delictivo[65].

Esta figura se regula para el agente encubierto en el terreno físico en el art. 282 bis LECrim. Si bien, hay que poner de manifiesto que en este art. en su apartado 4 se establece una lista de delitos que pueden ser cometidos por la delincuencia organizada, y se trata de un *numerus clausus*, esto es, una lista cerrada. Pero hay que decir que entendemos que tendría que tratarse de un *numerus apertus*, para así, evitar que delitos que también son cometidos por dichas organizaciones queden fuera, y en todo caso, para poder aplicar esta figura no solo en el terreno físico, sino en Internet, cuando se cometan delitos por tales organizaciones utilizando las nuevas tecnologías.

El Proyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, presentado por el Consejo de Ministros el 13 de Marzo de 2015, añade a este art. 282 bis dos nuevos apartados, el 6 y 7, en los que se regula esta figura del agente encubierto en Internet, y se amplía la lista de delitos en los que puede intervenir para esclarecer los hechos, incluyendo los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación. Asimismo se establece que el juez 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.

El ámbito delictivo en el que actúa este agente es en el seno de la delincuencia organizada, que se entiende como la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos de los que se establecen en este art.. Y hay que decir que se trata de una figura muy eficaz y efectiva para desmantelar estas organizaciones y redes criminales.

---

[64] BUENO DE MATA F., "Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿deberían ampliarse las actuales funciones del agente encubierto en Internet?", *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar el delito,* ed. La Ley, Madrid, 2012, págs. 315 y 316.

[65] 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, págs. 267-310.

El procedimiento que hay que seguir para que quepa la actuación de un agente encubierto se centra en varios puntos, que se establecen en ese art., y que suponen una garantía de control para esta figura, que puede lesionar derechos fundamentales. Estas garantías son:

- Autorización por el 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, para actuar bajo la identidad supuesta[66].

- Identidad supuesta 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 que va a infiltrarse necesita tener una identidad falsa para poder interactuar con los miembros de la organización, y no ser descubierto. Esta identidad falsa supone que su actuación se basa en el engaño de los delincuentes, proporcionándoles o intercambiando información o archivos con contenido delictivo, para ganarse su confianza y no levantar sospechas. Así, en la regulación que se hace de esta figura en el nuevo Proyecto de ley se establece la posibilidad de que el agente encubierto informático pueda intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los algoritmos asociados a dichos archivos ilícitos.

- Puesta a disposición de la información obtenido por el agente encubierto, a quien autorizó la investigación, a la mayor brevedad posible. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente.

[66] Observamos que se requieren una serie de requisitos, que son:
- La existencia de indicios suficientes de que se pueda estar cometiendo un delito.
- La idoneidad de la medida, esto es, valorar si va a resultar productiva, apta para obtener datos sobre la organización criminal.
- La necesidad o subsidiariedad de la medida, esto es, que es que es la única medida que permite obtener información sobre esa organización criminal.
- La gravedad de la conducta investigada, analizando las características de esa organización, y no solo el tipo delictivo y la pena que tiene prevista en el CP.
- Motivación suficiente, analizando el cumplimiento de los anteriores requisitos expuestos.

Además del control judicial, hay que hacer referencia también al control que se realiza por parte del supervisor, que es el responsable directo del agente siendo una especie de "protector" del funcionario, tendrá contacto con él y deberá saber interpretar las señales de alarma que aproximen su comportamiento al de los delincuentes que investiga, esto es, es el que determina la posibilidad de que el funcionario policial esté perdiendo su propia identidad y corra el riesgo de convertirse en uno más de la banda[67].

Una de las ventajas que tiene la actuación del agente encubierto en Internet, en comparación con la actuación del agente encubierto en el terreno físico, porque en este caso hay que construir todo una vida paralela irreal para la ocasión, mientras que en el caso de que actúe en la red solo se requiere un equipo informático, una conexión a Internet y un agente especializado que posea conocimientos informáticos que se ocupe de ello. Asimismo con la actuación del agente en la Red se asegura también la integridad de su vida y no habría posibilidades de cambio de bando. Además, se agilizaría la investigación, y al ayudarse de medios informáticos supone la posibilidad de valoración inmediata por parte del Juez[68].

En cuanto a los inconvenientes de esta diligencia encontramos el ya mencionado, esto es, que debería establecerse una lista abierta de delitos en los que se posibilitara actuar al agente encubierto, siempre que los delitos cometidos tengan la relevancia suficiente, y para permitir su actuación en la red. Lista que parece que en todo caso se amplía con el nuevo Proyecto de Ley Orgánica.

Además otro inconveniente de esta figura lo encontramos ante la testifical del agente en el proceso, que supone poner en peligro su vida, pues el hecho de que se obligue al agente encubierto a comparecer en el proceso que pudiera derivarse de los hechos en que hubieran intervenido, atenta contra su seguridad personal, tendría que comparecer por ejemplo el superior jerárquico para que no quedara su identidad al descubierto[69].

[67] DEL POZO PÉREZ M., "El agente encubierto…, op., cit., págs. 267-310.
[68] BUENO DE MATA F., *"Un centinela Virtual*…, op., cit., págs. 228 y 229.
[69] BUENO DE MATA F., *"Un centinela Virtual*…, op., cit., págs. 228 y 229.

3.6. VIRUS ESPÍA

Esta diligencia supone la posibilidad de utilizar por parte de los Cuerpos y Fuerzas de Seguridad del Estado, siempre bajo control judicial, el llamado virus "troyano" como técnica de investigación penal, utilizando así técnicas tradicionalmente empleadas para delinquir con fines lícitos, pues con ellos se busca esclarecer conductas delictivas[70].

Este virus "troyano" o "espía" es 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[71].

Supone, por tanto, la introducción de forma encubierta del virus en el ordenador del sospecho[72], sin su consentimiento, para obtener indicios y vigilar su actividad, lo que permite tener acceso a datos que almacena en el ordenador, al tráfico de entrada y salida de sus telecomunicaciones y de las páginas web que visita, toda esta información es transferida a agentes que deben haber sido autorizados por el Juez de Instrucción, que harán una copia para posteriormente poder analizarlos.

Hay que señalar que en todo caso estos virus que se crean con fines de investigación tienen que ser certificados, por si los creadores de los mismos no lo utilizan con estos fines, sino para lucrarse robando contraseñas, por ejemplo. Y uno de los estándares para la seguridad de la información más conocidos es la norma ISO-27001[73].

---

[70] CAMPANER MUÑOZ J., "¿Remote Forensic Software en España? Acerca de la Utilización de virus con fines de investigación en el proceso penal", *FODERTICS II: hacia una justicia 2.0*, ed. Ratio Legis, Salamanca, 2014, pág. 107.

[71] VELASCO NUÑEZ, E., "Novedades técnicas…, op., cit.

[72] Este programa puede introducirse de varias maneras en el ordenador del sospechoso:

- Cabe en primer lugar que los investigadores elaboren una página web con contenidos delictivos de señuelo, de manera que el virus alojado en esa página se instale en el ordenador de los que la visiten, o descarguen alguno de sus contenidos. Pero tiene como inconveniente que evoca la figura del delito provocado.
- Otra posibilidad es el envío de un correo electrónico que contenga un gusano oculto, pero presenta el problema de que se infecten los correos de la lista de contactos del sospechoso.
- O a través de la creación de una página web manipulada para dirigir la actividad del sospechoso para que acceda a la página y así se descargue el programa, pero presenta el inconveniente de que otros usuarios que no han sido dirigidos accedan y se contagien.
- La posibilidad más eficaz la inserción del mismo en un USB, que es la técnica más eficaz y segura, pero en este caso se presentan problemas en relación a su ejecución, pues supondría que los investigadores tuvieran que sustraerle un USB al sospechoso y devolvérselo posteriormente infectado, y no es fácil.

[73] CAMPANER MUÑOZ J., "¿*Remote Forensic*…, op., cit., pág. 108 y 111.

Esta técnica de intervención de las comunicaciones, que hasta ahora no gozaba de regulación, le resultaban de aplicación los arts. 579.1 y 580 a 588 de la LECrim, que aunque se refieren a la intervención de las comunicaciones postales y telegráficas, se pueden aplicar a cualquier tipo de comunicación. Pero el nuevo Proyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, presentado por el Consejo de Ministros el 13 de Marzo de 2015, lo regula expresamente en el art. 588 septies relativo a los registros remotos de equipos informáticos, que establece que tiene que ser autorizada por una resolución judicial motivada, y que debe establecerse con un límite temporal máximo de 3 meses, pues hay que tener en cuenta que supone una restricción de derechos, que puede vulnerar los recogidos en el art. 18 de la CE, pero no solo de la persona investigada, sino de otras ajenas al proceso que pueden ver lesionados sus derechos, si utilizan el dispositivo que está siendo monitorizado.

3.7. DRONES

Hay que empezar señalando que los drones son vehículos aéreos no tripulados, por ello también se conocen como VANT.

Su uso hay que encuadrarlo dentro del creciente empleo de la inteligencia artificial en la investigación penal, con fines de seguridad, para monitorizar sospechosos durante una investigación policial, pues permiten hacer fotografías aéreas con alta definición, ya que están provistos de potentes cámaras y sistemas de rastreo avanzados, pero estas aeronaves no tripuladas no sólo sirven para captar y almacenar imágenes, sino que pueden llegar incluso a hackear redes WiFi o a interceptar comunicaciones civiles, asimismo también nos encontramos con drones equipados con mecanismos de reconocimiento facial y toma de imágenes térmicas que ayudan a los entes policiales a detectar criminales. Por todo ello se han puesto de moda entre las Fuerzas y Cuerpos de Seguridad del Estado ya que es un sistema de vigilancia casi invisible y que puede permanecer en el aire durante mucho tiempo[74].

[74] BLASI CASAGRAN C., "El empleo emergente de drones con fines policiales en la Unión Europea: avances y limitaciones", editado por el Grupo de Estudios en Seguridad Internacional (GESI), Granada, 2014, publicado el 10/07/2014, en el link: http://www.seguridadinternacional.es/?q=es/content/el-empleo-emergente-de-drones-con-fines-policiales-en-la-uni%C3%B3n-europea-avances-y.

Teniendo en cuenta los usos que tienen, se pone de manifiesto que suponen una intrusión en los derechos fundamentales de la persona, relacionados con la privacidad, tales como el derecho al secreto de las comunicaciones y el derecho a la inviolabilidad del domicilio, pues para llevar a cabo esas labores de vigilancia van equipados con cámaras, cuentan con equipos de grabación de sonido, con cámaras de infrarrojos o sistemas de interceptación de las comunicaciones móviles, así como con detectores térmicos que tienen la posibilidad de utilizarlos para monitorizar 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 determinados parámetros tales como altura, edad, sexo o raza, con las implicaciones que supone para la privacidad[75].

Otro aspecto que hay que tener en cuenta en el uso de los drones es su invisibilidad, pues debido a su reducido tamaño y teniendo en cuenta la altura a la que vuelan son indetectables, y debido a las cámaras que llevan incorporadas pueden filmar y fotografiar cualquier cosa y a cualquier persona sin que nadie sea consciente de ello, lo que de nuevo puede vulnerar la privacidad de la persona.

Recientemente se aprobó la Ley 18/2014, de 15 de octubre, de medidas urgentes para el crecimiento, la competitividad y la eficiencia, que en la Sección 6.ª se refiere a las aeronaves civiles pilotadas por control remoto, pero que no regula la utilización de estos aparatos en la investigación penal. Se podía haber aprovechado esta ley para regular todas estas cuestiones controvertidas, pero sin embargo no se ha hecho. Y debido a los inconvenientes que tiene por su incidencia en la intimidad y privacidad de las personas se hace necesario definir unos límites y un marco de actuación.

Esta falta de regulación se ha intentado solventar en el nuevo Proyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal, presentado por el Consejo de Ministros el 13 de Marzo de 2015, pues en su art. 588 quinquies a. regula la captación de imágenes en lugares o espacios públicos, al establecer que "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 (…)".

[75] ACED FÉLEZ E., "Drones: una nueva era de la vigilancia y de la privacidad", *Revista Red Seguridad*, publicado en marzo de 2013, en el link: http://www.redseguridad.com/opinion/articulos/drones-una-nueva-era-de-la-vigilancia-y-de-la-privacidad

Pero deja todavía sin regular la utilización de estos dispositivos en lugares privados, por lo que de momento ha de entenderse que en todo caso quedará sometido a las mismas exigencias, esto es, si las grabaciones se llevan a cabo en espacios cerrados donde se desarrolla la intimidad y no se dispone del consentimiento del titular del espacio, será necesaria en todo caso la autorización judicial.

Asimismo hay que tener en cuenta que no pueden utilizarse los drones indiscriminadamente, sino solo en los casos en los que exista una razón de peso para recoger pruebas sobre un delito en concreto, y siempre que se haya pasado por un juicio de proporcionalidad por parte de la autoridad judicial en el que se pondere la seguridad y la lesión o vulneración a la privacidad o intimidad de los individuos[76].

Por último hay que señalar que si no se regula correctamente su uso podría ser utilizado por delincuentes, para inmiscuirse en la esfera personal de las víctimas, incluso dentro de sus domicilios.

3.8. POLÍGRAFO CEREBRAL (P300)

Para entender esta diligencia hay que empezar hablando de la actividad cerebral, que se basa en la propagación de impulsos eléctricos a lo largo de la membrana de la neurona y de sus prolongaciones, esta actividad eléctrica del cerebro es constante, y reacciona a estímulos, y son las modificaciones de esta actividad eléctrica cerebral provocadas por estímulos visuales, auditivos o táctiles las que se analizan, y se conocen como Potenciales Evocados Cognitivos[77].

El P300 es uno de estos Potenciales Evocados Cognitivos, y consiste en una onda positiva que se produce aproximadamente a los 300 milisegundos del inicio del estímulo que ha originado el potencial, estímulo que es la información que se le presenta. Esta prueba se desarrolla practicando un electroencefalograma, y si el sujeto al que se le presenta la información no la conocía no hay consecuencias en la actividad cerebral, pero si la conocía sí, esto es, la amplitud de la onda P300 se relaciona con la presencia en la memoria del sujeto de datos que previamente ya conocía. El registro de esta actividad cerebral es indoloro y no invasivo, pues se hace a través de unos sensores

[76] ACED FÉLEZ E., "Drones…, op., cit.

[77] ANDREU NICUESA C. Y VALDIZÁN USÓN J.R., "Potencial evocado cognitivo P300 en la investigación pericial", *Revista Aranzadi de derecho y proceso penal*, Nº. 33, 2014, págs. 345-366.

colocados en el cráneo del sujeto que registran los datos obtenidos para su posterior análisis[78].

Por lo tanto la prueba P300 es un método científico, que es útil en la investigación criminal, porque permite determinar quién conoce datos del delito detectando la respuesta del cerebro cuando se le presentan a un sujeto relacionado con el delito que se pretende investigar una información que ya tenía con anterioridad[79]. Se aplica en la búsqueda de datos almacenados en el cerebro de sospechosos o testigos que, siendo desconocidos para los investigadores, pueden sin embargo contribuir al avance de la investigación criminal y a la resolución de los casos, no se utiliza como un detector de mentiras[80].

Así, esta actividad cerebral que mide la P300 puede orientar la investigación en el hallazgo de nuevas pruebas físicas, los resultados que se obtienen con la prueba P300 no afectan al procedimiento judicial ni a la garantía de presunción de inocencia, solo podrán hacerlo las pruebas físicas que puedan hallarse derivadas del análisis de resultados de la P300. Por lo que la utilización de esta diligencia no es como prueba de culpabilidad, como medio de prueba, sino que se pretende la búsqueda de datos útiles para la investigación pruebas materiales que sí puedan constituirse como tales, esto es, se pretende su utilización como indicio[81].

En este mismo sentido hay que apuntar que su uso es residual y subsidiario, para los casos en los que no hay más vías para seguir investigando.

Los avances en neurociencias ponen a disposición de la investigación penal nuevas técnicas, como es esta P300; ahora bien, hay que decir que esta diligencia presenta algunos puntos cuestionables[82]:

- La posible afectación al derecho a no declarar contra sí mismo (art. 24.2 de la CE), pero al analizar el uso que se hace de esta diligencia se pone de relieve que no se requiere ningún respuesta verbal por parte del sujeto por lo que

[78] VILLAMARÍN LÓPEZ M.L., "La búsqueda de la verdad en el proceso penal a través de las nuevas tecnologías: a propósito del polígrafo cerebral", *FODERTICS 3.0: estudios sobre nuevas tecnologías y justicia*, ed. Comares, Granada, 2015, págs. 175 y 176.
[79] ANDREU NICUESA C. Y VALDIZÁN USÓN J.R., "Potencial evocado…, op., cit., págs. 345-366.
[80] VILLAMARÍN LÓPEZ M.L., "La búsqueda…, op., cit., pág. 176.
[81] ANDREU NICUESA C. Y VALDIZÁN USÓN J.R., "Potencial evocado…, op., cit., págs. 345-366.
[82] ANDREU NICUESA C. Y VALDIZÁN USÓN J.R., "Potencial evocado…, op., cit., págs. 345-366.

no supone un riesgo contra el derecho a no declarar, sino que únicamente el experto perito valora la reacción neurofisiológica como reacción al estímulo.

- La posible manipulación de la respuesta, ahora bien, en relación a este punto, hay que tener presente que los potenciales evocados cognitivos no se puede modificar por la voluntad del sujeto, por lo que no cabe tal manipulación.

Actualmente no goza de regulación legal, pero podría encajarse en la doctrina de las intervenciones corporales, pues en este sentido, el art. 363 de la LECrim., dice que "los Juzgados y Tribunales ordenarán la práctica de los análisis químicos únicamente en los casos en que se consideren absolutamente indispensables para la necesaria investigación judicial y la recta administración de justicia. (…) A tal fin, podrá decidir la práctica de aquellos actos de inspección, reconocimiento o intervención corporal que resulten adecuados a los principios de proporcionalidad y razonabilidad".

Pero se hace necesaria una mayor regulación, y más detallada, pues está claro que cabe su práctica cuando media el consentimiento del sujeto prestado con todas la garantías y en presencia de su abogado, pero ¿puede realizarse en contra de la voluntad del sujeto aunque medie autorización judicial? Observamos que se plantea el mismo problema que con la toma de muestras de ADN[83].

Es una técnica muy reciente, que casi no se conoce, y que sería un buen momento de regularla en el nuevo Proyecto de Reforma de la Ley de Enjuiciamiento Criminal, debido a que genera una gran expectación mediática y tiene una gran repercusión práctica, así como detractores que amparándose en la vulneración de los derechos fundamentales constitucionalizados, no abalan su utilización[84].

[83] VILLAMARÍN LÓPEZ M.L., "La búsqueda…, op., cit., págs. 180 y 181.
[84] En este punto cabe mencionar a BALLESTÍN MIGUEL, A., Magistrado de la Audiencia Provincial de Zaragoza, en el artículo: "P300: Inhumanizando la justicia", *Revista Adalán*, publicado el 28/02/2014, en el link: http://www.andalan.es/?p=8878.

4. CONCLUSIONES

Tras la elaboración del Trabajo Fin de Grado sobre las diligencias que se están utilizando en la investigación de los delitos cometidos a través de las nuevas tecnologías, podemos concluir que:

1. Estos delitos cometidos a través de Internet presentan unas características especiales, la facilidad de comisión por el autor, que desarrolla la conducta delictiva en cuestión de segundos y sin riesgo; la impunidad, pues se esconden y ocultan en la Red; la masividad y trasnacionalidad, ya que pueden afectar a muchas personas, independientemente de donde se encuentren, e igualmente pueden afectar de forma simultánea a una pluralidad de personas en diferentes puntos del planeta; y la gravedad de las conductas delictivas que lesionan de forma mucho más grave bienes jurídicos protegidos.

2. Debido a la especialidad de estos delitos y de las diligencias que se utilizan en su investigación, se ha hecho necesaria la creación, dentro de la Policía Nacional y de la Guardia Civil, de dos grupos especializados en la persecución de estos delitos, y compuestos por personal especializado en informática para facilitar el desarrollo de tales diligencias. Asimismo se ha tenido en cuenta para su creación la proliferación de estos delitos que se ha producido y está produciendo en las últimas décadas.

3. En cuanto a la competencia para conocer de estos delitos hay que tener en cuenta que estos delitos tienen carácter transfronterizo, por lo que es competente para conocer de ellos cualquier órgano jurisdiccional del lugar en el que se haya evidenciado la exteriorización de los efectos del delito, esto se conoce como principio de ubicuidad. Ahora bien, si se conoce el concreto lugar de comisión será el juez de ese lugar el que se atribuya la competencia conforme al criterio general de atribución de competencia que es el *forum delicti comisi*.

4. En este mismo sentido debido a la trasnacionalidad de las conductas delictivas, es esencial promover la cooperación judicial internacional, para conseguir una coordinación entre los distintos países, pues no hay que perder de vista que estos delitos se suelen cometer por grupos organizados que actúan a escala mundial, por lo que se hace necesaria una armonización de todas las legislaciones, para permitir así la persecución eficaz de estos delitos.

5. En relación a las diligencias policiales utilizadas para investigar estos delitos cometidos a través de Internet, se extrae la conclusión de que en el desarrollo de todas ellas se afecta a los derechos fundamentales del art. 18 de la CE, que son el derecho a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones. Por ello, se hace necesario establecer unas garantías de control que se concretan en requerir a las Fuerzas y Cuerpos de Seguridad del Estado una autorización judicial previa para entender que su desarrollo es legal, y establecer un límite temporal para evitar que la vulneración se prolongue indefinidamente.

6. Hasta ahora era patente una falta de regulación legal de estas diligencias, siendo desde luego insuficiente el escaso encaje legal que se le encontraba en la LECrim. Este problema parece no obstante subsanado con el esperado Proyecto de Ley Orgánica de Modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, presentado por el Consejo de Ministros el 13 de Marzo de 2015, pues instrumenta algunas de estas diligencias, y supone un claro avance ya que va a permitir configurar y definir el marco de actuación en la investigación criminal de estos nuevos delitos cometidos a través de Internet.

7. A pesar de esta esperada regulación, todavía quedan cuestiones importantes por regular, tales como el protocolo de actuación para la custodia de muestras de ADN, o la novedosa diligencia conocida como P300, tampoco se adapta a las nuevas tecnologías la diligencia de la entrega vigilada. Por lo que esta futura regulación tan esperada se prevé aún insuficiente para abordar los nuevos retos que se plantean.

BIBLIOGRAFÍA

ACED FÉLEZ E., "Drones: una nueva era de la vigilancia y de la privacidad", *Revista Red Seguridad*, publicado en marzo de 2013, en el link: http://www.redseguridad.com/opinion/articulos/drones-una-nueva-era-de-la-vigilancia-y-de-la-privacidad

ALDAMA SAÍNZ C., "Vulnerabilidades en periciales informáticas", *FODERTICS II: hacia una justicia 2.0. Estudios sobre derecho y nuevas tecnologías*, ed. Ratio Legis, Salamanca, 2014.

ANDREU NICUESA C. Y VALDIZÁN USÓN J.R., "Potencial evocado cognitivo P300 en la investigación pericial", *Revista Aranzadi de derecho y proceso penal*, Nº. 33, 2014.

BALLESTÍN MIGUEL A., "P300: Inhumanizando la justicia", *Revista Adalán*, publicado el 28/02/2014, en el link: http://www.andalan.es/?p=8878.

BLASI CASAGRAN C., "El empleo emergente de drones con fines policiales en la Unión Europea: avances y limitaciones", editado por el Grupo de Estudios en Seguridad Internacional (GESI), Granada, 2014, publicado el 10/07/2014, en el link: 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., "Ciberterrorismo: tratamiento procesal y penal del terrorismo del futuro", *Estudios actuales en derecho y ciencia política: [2º. Encuentro INCIJUP]*, ed. Andavira, Santiago de Compostela, 2013.

BUENO DE MATA F., "Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿deberían ampliarse las actuales funciones del agente encubierto en Internet?", *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar el delito,* ed. La Ley, Madrid, 2012.

BUENO DE MATA F., *Prueba electrónica y proceso 2.0*, ed. Tirant lo Blanch, Valencia, 2014.

BUENO DE MATA, F., "Nuevas tecnologías y diligencias", *FODERTICS, estudios sobre derecho y nuevas tecnologías*, ed. Andavira, Santiago de Compostela, 2012.

BUJOSA VADELL L.M., "Introducción", *FODERTICS II: hacia una justicia 2.0. Estudios sobre derecho y nuevas tecnologías,* ed. Ratio Legis, Salamanca, 2014.

CABEZUDO BAJO M.J., "La regulación del "uso forense de la tecnología del ADN" en España y en la UE", *FODERTICS, estudios sobre derecho y nuevas tecnologías*, ed. Andavira, Santiago de Compostela, 2012.

CAMPANER MUÑOZ J., "¿Remote Forensic Software en España? Acerca de la Utilización de virus con fines de investigación en el proceso penal", *FODERTICS II: hacia una justicia 2.0*, ed. Ratio Legis, Salamanca, 2014.

DEL POZO PÉREZ M., "Algunas cuestiones polémicas sobre el ADN y el proceso penal", *Revista general de derecho público comparado*, Nº 10, 2012.

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.

"Encuentro con… Manuel Vázquez López, Comisario Jefe de la Brigada de Investigación Tecnológica de la Policía", *Revista Dintel*, nº 28, Madrid, número especial AGE 2008/2009, disponible en el link: http://www.revistadintel.es/Revista1 /DocsNum 28/Encuentro/Vazquez.pdf.

FERNÁNDEZ LÁZARO, F., "La Brigada de Investigación Tecnológica: la Investigación policial, *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, ed. Consejo General del Poder Judicial, Madrid, 2006.

GÓMEZ TOMILLO M., "Responsabilidad penal por delitos contra la propiedad intelectual cometidos a través de Internet", *La propiedad intelectual en la era digital. Límites e infracciones a los derechos de autor en Internet*, ed. La Ley, Madrid, 2011.

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, Madrid, 2013.

ORTIZ PRADILLO, J.C., "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar el delito*, ed. La Ley, Madrid, 2012.

PÉREZ GAIPO J., "Intervención de las comunicaciones, nuevas tecnologías y derechos procesales: viejos principios para nuevas realidades", *FODERTICS II: hacia una justicia 2.0*, ed. Ratio Legis, Salamanca, 2014.

SALOMON CLOTET, J., "Delito informático y su investigación", *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, ed. Consejo General del Poder Judicial, Madrid, 2006.

SERRANO SANTOYO A. y MARTINEZ MARTÍNEZ E., *La Brecha Digital: Mitos y Realidades*, ed. UABC, México, 2003.

VELASCO NUÑEZ, E., "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías", *Revista digital El Derecho*, publicado el 24/02/2011, en el link: http://www.elderecho.com/penal/Novedades-tecnicas-investigacion-vinculadastecnologias _ 11_237430010.html.

VELASCO NÚÑEZ, E., *Delitos cometidos a través de Internet: cuestiones procesales*, ed. La Ley, Madrid, 2010.

VILLAMARÍN LÓPEZ M.L., "La búsqueda de la verdad en el proceso penal a través de las nuevas tecnologías: a propósito del polígrafo cerebral", *FODERTICS 3.0: estudios sobre nuevas tecnologías y justicia*, ed. Comares, Granada, 2015.

PÁGINAS WEB

BIT – Funciones, consultado el 15 de Febrero de 2015, disponible en el link: http://www.policia.es/org_ central/judicial/udef/bit_alertas.html.

El proceso de clonación, consultado el 3 de marzo de 2015, disponible en el link: http://www. ondataforensic.com/proceso-de-clonacion.php.

La Unidad, consultado el 15 de febrero de 2015, disponible en el link: https://www.gdt. guardiacivil.es/webgdt/la_unidad.php.

LEGISLACIÓN Y DOCUMENTACIÓN DE INSTITUCIONES JURÍDICAS

- Proyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, presentado por el Consejo de Ministros el 13 de Marzo de 2015.
- Ley 18/2014, de 15 de octubre, de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
- *La Estrategia de Ciberseguridad Nacional*, 2013, consultada el 11 de abril de 2015, disponible en el link: http://www.lamoncloa.gob.es/documents/20131332 estrategiade ciberseguridadx.pdf
- Instrucción nº 1/2008 sobre la dirección por el Ministerio Fiscal de las actuaciones de la Policía Judicial, Capítulo VI: Las distintas fases de actuación de la Policía Judicial.
- Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir de ADN.
- Convenio sobre Ciberdelincuencia hecho en Budapest el 23 de noviembre de 2001.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
- Constitución Española, 1978.
- Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal.

JURISPRUDENCIA

- Acuerdo de la Sala de lo Penal del TS, de 24 de septiembre de 2014.
- STC 173/2011, de 7 de noviembre.
- STS de 6 de junio de 2011.
- STS de 5 de noviembre de 2009.
- STS de 28 de enero de 2009.

- STS de 19 de diciembre de 2008.
- STS de 28 de mayo de 2008.
- STS de 5 de febrero de 2008.