ESCUELA DE PRÁCTICA JURÍDICA
SALAMANCA

TRABAJO FIN DE TÍTULO

MÁSTER EN ACCESO A LA ABOGACÍA

Curso 2015/2017

EL USO DE VIRUS ESPÍA COMO DILIGENCIA DE INVESTIGACIÓN: ANALISIS CRÍTICO Y PROPUESTAS

Nombre de la estudiante: Sara Jorge Sanmartín

Tutor: Federico Bueno de Mata

Mes: diciembre **Año: 2016**

TRABAJO FIN DE TÍTULO

MÁSTER EN ACCESO A LA ABOGACÍA

EL USO DE VIRUS ESPÍA COMO DILIGENCIA DE INVESTIGACIÓN: ANALISIS CRÍTICO Y PROPUESTAS

THE USE OF SPYWARE AS A DILIGENCE OF INVESTIGATION: CRITICAL ANALYSIS AND PROPOSALS

Nombre de la estudiante: Sara Jorge Sanmartín
e-mail de la estudiante: sarajosan@usal.es

Tutor: Federico Bueno de Mata

RESUMEN

El avance de las nuevas tecnologías y la proliferación de los medios de comunicación telemáticos han traído como consecuencia la creación de nuevos delitos así como novedosas formas de comisión de los delitos tradicionales.
Este fenómeno, conocido como cibercrimen o ciberdelincuencia ha exigido una respuesta por parte de las fuerzas represoras, que adaptándose también al actual escenario tecnológico, ha innovado en la labor de investigación y represión de estos delitos. El panorama legislativo tanto del derecho español como del derecho comparado se hace eco de estas circunstancias, destacando como el avance más importante y actual, la entrada en vigor de la Ley 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, texto legal que incluye el uso de los virus espía como diligencia de investigación. Junto al desarrollo legislativo nos centraremos en la ejecución de las diligencias contempladas en la Ley y en la concreta preparación de los cuerpos y fuerzas de seguridad para acabar incidiendo en los ámbitos en los que aún quedan retos pendientes para lograr una regulación más coherente eficaz y desde la máxima garantía a los Derechos Fundamentales del investigado.

PALABRAS CLAVE: virus espía, diligencia, cadena de custodia, prueba electrónica.

ABSTRACT

The advance on new technologies and the proliferation of telematics media have led not only to the creation of new crimes but also to new ways of commission from traditional crimes. This fact, known as cybercrime, has required a response from the repressive forces, which have been adapted to the current technological sector, innovating in the investigation and repression of these crimes.
The legislative overview from both, Spanish and comparative law, takes into account these circumstances, highlighting the entry into force of Law 13/2015 as the most important and current progress, amending the Criminal Procedure Law in favour of the strengthening of procedural guarantees and the regulation of technological research measures in a legal text that includes the use of spywares as an investigation procedure.
Together with the legislative development, we will focus on the implementation of the procedures contemplated in the Law and on the concrete preparation of the security forces to end up focusing on the areas in which there are still pending challenges in order to achieve a more coherent and efficient regulation, guaranteeing the Fundamental Rights of the investigated.

KEYWORDS: spyware, procedure, chain of custody, electronic evidence.

ÍNDICE

ABREVIATURAS

BIT:	Brigada de Investigación Tecnológica
CE:	Constitución Española
CNP:	Cuerpo Nacional de Policía
EC3:	European Cybercrime Centre
LECRIM:	Ley de Enjuiciamiento Criminal
LO:	Ley Orgánica
LOPJ:	Ley Orgánica del Poder Judicial
TIC:	Tecnologías de la información y la comunicación
UE:	Unión Europea

INTRODUCIÓN

El uso de virus espía como diligencia de investigación policial es una medida implantada recientemente en nuestra Ley de Enjuiciamiento Criminal mediante la Promulgación de la Ley Orgánica 13/2015, ley que a pesar de sus indiscutibles ventajas y el progreso normativo que ha supuesto ya ha cosechado sus primeras críticas entre los autores entendidos en la materia. El desarrollo de las nuevas tecnologías y el avance en materia de comunicaciones, la creación de dispositivos y el desarrollo y ampliación de las funciones de los equipos informáticos han traído consigo la aparición de nuevos delitos y ha supuesto un cambio en la forma de comisión de otros, se trata del fenómeno conocido como cibercrimen. La aparición del cibercrimen o ciberdelincuencia ha exigido una respuesta represiva del Derecho. Por este motivo ha sido imprescindible renovar también las formas de prevención, investigación y contención de estas conductas, siendo necesario para ello una formación especializada de los cuerpos de seguridad. De esto modo se ha ido llevando a cabo la creación de órganos y unidades especializadas, tanto a nivel nacional como internacional. Sin embargo tanto este como otros cambios necesita encontrar su previsión y amparo en la ley. Con un panorama legislativo enfocado a la regulación de la comisión "física" de delitos "tradicionales", dejando fuera la interacción entre delincuencia y tecnologías de la información y la comunicación, también ha sido indispensable la reforma, por un lado, de ciertas leyes y la creación de otras.

Este trabajo se centra en la diligencia de investigación consistente en el empleo de virus espía para la averiguación de delitos. Veremos como la ley ha tratado de regular nuevas medidas de acción para el control de una nueva realidad: la necesidad en determinadas ocasiones de adentrarse de forma remota el ordenador de una persona sin el consentimiento ni conocimiento de esta. Haremos un estudio de las distintas variantes que han existido y que existen en la actualidad para ejecutar este tipo de medida así como el alcance de cada de ellas. Veremos las consecuencias de esta nueva regulación y del uso práctico de los virus espía siendo la más relevante de todas ellas la afectación a los Derechos Fundamentales a la protección de datos, a la intimidad personal y familiar, al secreto de las comunicaciones y a la inviolabilidad del domicilio. Al ser esta una diligencia que afecta tan directamente a importantísimos Derechos Fundamentales del ser humano solo podrá recurrirse a esta bajo unos determinados presupuestos y respetando siempre los principios rectores de nuestro ordenamiento jurídico. Sin embargo no todo lo referente al uso de *softwares* espías podemos encontrarlo claramente regulado en la ley. Debido a que existen ciertas cuestiones que no han sido aún esclarecidas en textos legales tendremos que dar una visión de cómo se opera en la práctica. De este modo, no solo en el plano legislativo podemos ver reflejada la necesidad de adaptarse al a los progresos electrónicos y

tecnológicos. El poder judicial ha sido también uno de los más afectados por estos cambios y se ha encontrado en la necesidad de enjuiciar ante lagunas jurídicas del tal mido que ciertos vacios han podido ser colmados mediante la jurisprudencia y la práctica jurídica. Siendo esta una materia con un alcance tan grande haremos un repaso de los fronteras que la ley establece para salvaguardar las garantías propias de un estado de derecho, empezando por los requisitos que se exigen para poder emplear este tipo de medidas y hasta las limites que se imponen a la actuación policial con el objeto de que la injerencia a los Derechos Fundamentales de los ciudadanos sea la menor posible. Nuevamente en este punto tendremos que recurrir a la visión judicial ya que la ponderación realizada por jueces y tribunales entre Derechos Fundamentales y otro tipo de intereses esenciales para resolver cada caso concreto respetando el delicado equilibrio entre la libertad de los ciudadanos y la necesidad de perseguir y reprimir las conductas criminales.

Existen cuestiones vitales a atender comprendidas entre la investigación del delito y el enjuiciamiento del mismo. Me estoy refiriendo a la obtención y aseguramiento de pruebas que al igual que otras cuestiones ya mencionadas revisten peculiaridades cuando nos movemos en el plano de las diligencias de investigación tecnológicas. En este sentido la materia gira en torno al concepto de prueba electrónica un tipo de prueba que por sus características intrínsecas arroja claridad y certeza pero cuya volatilidad supone un importante problema a la hora de garantizar su conservación inalterada. La cadena de custodia se convierte así en una parte del proceso fundamental y paradójicamente uno de los extremos más carentes de concreción normativa que podemos encontrar en este ámbito. Por este motivo deberemos recurrir nuevamente a la visión práctica de la cadena de custodia, reflejando como se lleva a cabo la misma en la actualidad, a la construcción jurisprudencial que se ido desarrollando del concepto y a la visión doctrinal del mismo arrojada por distintos autores. También veremos cómo está configurada la cadena de custodia en otros países y mediante este compendio trataremos de recoger propuestas para una nueva regulación que acabe con la inseguridad jurídica probatoria.

A continuación expondré en este trabajo quiénes son y cómo se estructuran los cuerpos de seguridad a nivel nacional, europeo y extranjero, el marco normativo existente en la materia deteniéndome especialmente en la LO 13/2015. Se hará un estudio detallado de virus informáticos como diligencia de investigación abordando para ello el concepto, la tipología y los presupuestos de uso para terminar aproximándonos al el tema desde una perspectiva e la ejecución policial. Por último se aportará, mediante un anexo una propuesta de protocolo de cadena de custodia para la prueba obtenida en estas diligencias.

1. EL CNP Y LA LUCHA CONTRA EL CIBRECRIMEN ESPECIAL ATENCIÓN A LA BIT Y A LA FORMACIÓN ESPECIALIZADA

En los últimos años hemos sido testigos de un crecimiento en el plano de los avances tecnológicos sin precedentes. La creación de nuevos softwares informáticos, el desarrollo de nuevos equipos más potentes y capaces de procesar más información y la creación de nuevas líneas comunicativas son algunos de los progresos más reseñables. Estos progresos no son solo cualitativos si no también cuantitativos de tal modo que se ha multiplicado el número de dispositivos existentes. Tanto es así que se ha comenzado a escuchar hablar del *internet de las cosas* (IoT)[1] un término referido para predecir una realidad que muchos consideran que no tardará en llegar a nuestras vidas y consistente en ampliar la red no solo a los dispositivos electrónicos si no a todo tipo de objetos cotidianos de modo que toda nuestra vida estaría "conectada a internet" El desarrollo de las nuevas tecnologías ha traído consigo números avances en un gran número de ámbitos, sin embargo, inevitablemente, no todas las repercusiones del mismo han sido positivas. La criminalidad ha encontrado nuevas formas de expansión y de comisión de delitos y ante esto el derecho ha tenido que reaccionar.

Dentro de la dirección general de policía, o cuerpo nacional de policía (CNP)[2] podemos encontrar, como órgano directivo, a la policía judicial, dependiente a esta encontramos a la Unidad de Delincuencia Económica y Financiera (UDEF) quien a su vez dirige a la Brigada de Investigación Tecnológica. Como puede deducirse fácilmente de su nombre esta será la unidad especializada dentro del cuerpo nacional de policía de luchar contra el cibercrimen. La brigada se desarrolló a la par que los avances tecnológicos y la evolución y expansión de internet aunque no fue la pionera en este ámbito. Su predecesor nació en el año 1995 y fue el Grupo de Delitos Informáticos de la Brigada de Delincuencia Económica y Financiera (BDEF), idea que pronto fue asumida por la guardia civil ya que en el año 1996 crearon el Grupo de delitos telemáticos. No fue hasta 2002 cuando, debido al crecimiento y división en subgrupos operativos del BDEF, que esta unidad se transformo en la Brigada de Investigación Tecnológica.

Esta unidad tiene como funciones más destacables las de investigación, formación de personal del propio CNP y de otros organismos semejantes, coordinación de operaciones, así

[1] IoT viene de las siglas en inglés Internet Of Things sería una forma de "conectar" (a internet) el máximo de objetos que nos rodean, entre ellos y con nosotros" http://www.xataka.com/internet-of-things/las-3-tecnologias-clave-para-el-internet-de-las-cosas fecha de consulta 15 de agosto de 2016

[2] El CNP, se define así mismo en su página web como: "La Policía Nacional es un instituto armado de naturaleza civil, con estructura jerarquizada que tiene como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana, con ámbito de actuación en todo el territorio nacional." http://www.policia.es/cnp/cnp.html fecha de consulta 15 de agosto de 2016

como su coordinación y ejecución en el plano internacional.[3] La organización de la BIT se estructura en tres secciones [4] dedicadas a distintos ámbitos de actuación que expondremos a continuación.

La primera sección originariamente estaba enfocada a la persecución de delitos que por un lado atenten contra uno de los bienes jurídicos más atacados por la ciberdelincuencia: la protección del menor y por otro lado crímenes que dañen el derecho fundamental a la intimidad de las personas. La integridad del menor se trata de salvaguardar luchando contra tipos delictivos de pornografía infantil (en cualquiera de sus ámbitos, creación, distribución o tenencia) y delitos de bullying[5] y grooming (al que nos referiremos más adelante). Recientemente se ha creado otro foco de actuación dentro de esta primera sección destinado un rastreo permanente de la red en busca de tipos delictivos con el objeto de alertar a la autoridad correspondiente según los concretos hechos detectados, hablamos del llamado Grupo de Redes Abiertas y destaca especialmente por su faceta de colaboración mediante la elaboración de informes sobre nuevos *modus operandi*.

La segunda sección también tiene divididas sus competencias. Por un lado cuenta con dos grupos dedicados combatir los fraudes en la red, un grupo para luchar contra los delitos puramente informáticos y un último grupo dedicado a la protección de la propiedad intelectual e industrial. Respecto a la lucha contra el fraude en la red conviene mencionar algunos ejemplos que nos permitan formarnos una idea más concreta de en qué consisten este tipo de hechos. Debe comenzarse indicando que prácticamente todas estas conductas son distintos tipos de comisión del delito de estafa[6]. Uno de los fraudes más típicos en internet son las falsas compraventas (obtención de una retribución económica por un bien que se ofrece en la red y que nunca llega a entregarse al comprador). Muy relacionadas con este se encuentran aquellas conductas basadas en la oferta de trabajo falsa, en la que el ciberdelincuente obtiene su provecho económico solicitando al aceptante de trabajo anticipos de dinero para la ejecución de trámites de contratación o bien utilizando al "trabajador" como intermediario para la comisión de otros hechos delictivos. En los últimos años han cobrado mucha fuerza también los delitos de

[3] http://www.policia.es/org_central/judicial/udef/bit_funciones.html fecha de consulta 15 de agosto de 2016

[4] RIVERO J., 2008-2009 Entrevista a Manuel Vázquez López Comisario Jefe de la Brigada de Investigación Tecnológica de la Policía, *nº28, a+*, pág. 33-38

[5] Bullying es un término empleado para hacer referencia al acoso escolar, es decir, a cualquier modalidad de agresión física o psíquica que un escolar ejerza sobre otro siempre que está situación de alargue en el tiempo.

[6] El artículo 248.1 del código penal recoge la definición del tipo básico del delito de estafa (el cual se amplia y concreta en el artículo 248.2): "Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno."

phishing[7], es decir los delitos basados en la obtención de claves y contraseñas que permitan acceder a daros personales y bancarios de los usuarios.

Para finalizar, la tercera sección no persigue un tipo de delito si no que se encarga de la formación especializada, por ello recibe el nombre de sección técnica. Entre sus funciones más destacables podemos encontrar las siguientes: en primer lugar realiza labores de asistencia al resto de secciones que componente la BIT y a otras unidades del CNP, también lleva a cabo la formación de agentes de policía tanto a nivel nacional como internacional manteniendo comunicaciones constantes con instituciones como el Consejo de Europa, Europol o Interpol y por último se encarga de potenciar el I+i+D [8] en la investigación tecnológica.

En base a esto es evidente que la preparación de sus agentes debe ser, consecuentemente, amplia. Esto supone quela formación va más allá de una instrucción policial común si no que se requieren conocimientos en el campo de las nuevas tecnologías. Al aprendizaje continuo es la forma de garantizar estos conocimientos en un campo que se encuentra en constante evolución. El factor psicológico de los agentes no es menos relevante. Debe tratarse de personas con una fuerte resistencia emocional capaces de lidiar con delitos de aterradora naturaleza. Es por esta razón que ya se ha instaurado, en algunos países europeos, como medida la realización de test psicológicos a los agentes y la rotación de los mismos por distintas unidades a modo de evitar una sobreexposición dañina para su salud psicológica.[9]

A nivel europeo también existen especialidades para el tratamiento y la persecución de este tipo de conductas delictivas. Una de las más relevantes es el European Cybercrime Centre (EC3) su objetivo principal es la lucha contra la delincuencia enfocada desde una perspectiva tanto directa como indirecta, al ser pionero en la creación de nuevos estudios de investigación de acerca de distintas técnicas informáticas.

---

[7] Una especialidad aún más difícil de combatir del phishing es el llamado pharming, el cual no requiere actuación alguna por parte del usuario ya que se emplean determinados software maliciosos que redirigen al usuario en la web para el robo de información.

[8] "I+D+I o lo que es lo mismo Investigación, desarrollo e innovación , es un nuevo concepto de investigación adaptado a los estudios relacionados con el avance tecnológico e investigativo centrados en el avance de la sociedad, siendo una de las partes más importantes dentro de las tecnologías informativas." http://www.plannacionalidi.es/que-es-idi/ fecha de consulta 20 de agosto de 2016

[9] Así lo declaro D. JUAN MIGUEL MANZANAS MANZANA, jefe de la Brigada de Investigación Tecnológica en la comisaría general de la policía judicial de la dirección general de la policía, durante su comparecencia del en la Ponencia conjunta de estudio sobre los riesgos derivados del uso de la red por parte de los menores, celebrada el día 16 de mayo de 2013. Este además explicó "las personas que están aquí dedicadas tienen –cómo les diría–, se encuentran sometidas a una presión especial. Quiero decir, que estar viendo y buscando determinadas imágenes de este tipo tan aberrantes supone a veces, depende de cada persona y su situación, personal, familiar y demás, puede suponer una carga importante." http://www.senado.es/web/expedientficblobservlet?legis=10&id=5a fecha de consulta 10 de agosto de 2016

Otro de los fines perseguidos por el EC3 es el fomento de la colaboración internacional, muy necesaria siendo el cibercriminal un delito sustancialmente transfronterizo. Los acciones ilegales llevadas a cabo en internet son acciones *per se*, internacionales[10] a causa de las características propias de la comunicación telemática a través de la red. Sin embargo lograr un alto grado de cooperación entre países a menudo puede resultar una tarea complicada. Es por esto motivo que el centro cuenta con el apoyo de una serie de organismos colaboradores.[11] Entre ellos podemos destacar la Agencia Europea de Seguridad en Redes e Información (*European Network and Information Security Agency* o ENISA) o el Centro de Conocimientos Especializados para la Seguridad Cibernética en Europa[12]. También resultan relevantes el Grupo de Trabajo de la Unión Europea en la Lucha contra la Ciberdelincuencia (European Union Cybercrime Taskforce o EUCTF) o la Organización Internacional de Policía Criminal (*International Criminal Police Organization* o INTERPOL), encargada, (como ella misma declara en su página web) de *"*permitir que las policías de todo el planeta colaboren*"*[13]. Por último cabe añadir a la lista a la Unidad de Cooperación Judicial de la Unión Europea (*European Union's Judicial Cooperation Unit* o EUROJUST) cuya función es *"*apoya la coordinación y cooperación judiciales entre las autoridades nacionales en la lucha contra la delincuencia organizada grave que afecte a más de un país de la UE. *"*[14]

Por su parte el EC3 enfoca gran parte de sus esfuerzos a la vertiente de la prevención de la ciberdelincuencia asesorando así a las posibles víctimas del cibercrimen a fin de luchar contra la comisión de hechos delictivos desde el origen, esto es, tratando de evitar la comisión de delitos. Es por este motivo que el EC3 basa sus previsiones y diseña sus mecanismos de prevención del cibercrimen en torno al Proyecto 2020, un estudio llevado a cabo por la Alianza Internacional de Protección para la Ciberseguridad (ICSPA). Se trata de un estudio dirigido por EUROPOL, y que recoge informaciones aportadas tanto por organismos de seguridad como por los miembros de ICSPA. El proyecto 2020 trata de arrojar una visión de futuro acerca de cómo evolucionará la ciberdelincuencia en los próximos años. Así por ejemplo señala como ámbitos en los que actuará la criminalidad la alteración de redes de información, la intrusión monetaria,

---

[10] LOPEZ, A. "La investigación policial en Internet: estructuras de cooperación internacional* Monográfico III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas", nº5 *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, 2007, PÁG. 69: explica que; "al mencionar su carácter per se quiere significarse que no existe una diferencia esencial entre el uso de una máquina en Austria de una en Australia, es decir, que no existe ningún factor local de gran relevancia (salvo el del idioma). Así, el terreno de juego es el mundo entero, desvirtuando, en cierto modo, el principio de territorialidad del Derecho."

[11] AGUILAR, M. M. (2015). Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. *Revista Criminalidad*, 57 (1), págs. 121-135.

[12] http://europa.eu/abouteu/agencies/regulatory_agencies_bodies/policy_agencies/enisa/index_es.htm

[13] http://www.interpol.int/es/Acerca-de-INTERPOL/Visi%C3%B3n-de-conjunto

[14] http://europa.eu/abouteu/agencies/regulatory_agencies_bodies/pol_agencies/eurojust/index_es.htm

la evasión fiscal, el acceso y posterior destrucción a determinados datos, o la falsificación de acreditaciones de identidad y de moneda.[15]

Para finalizar no podemos pasar por alto a otro de los organismos más importantes en la materia, este es EUROPOL, organismo similar a la ya mencionada INTERPOL pero a nivel europeo. Creado en 1999 y con sede en La Haya, EUROPOL es una *"*Agencia encargada de velar por el cumplimiento de la ley en la UE*"*[16]. Se trata de un centro de conocimientos enfocado hacia la colaboración internacional y el intercambio de información. Los concretos objetivos que en cada comento asume el grupo se reflejan anualmente en el "programa de trabajo anual de EUROPOL" y dependen de las específicas necesidades que se considere que se dan cada año. Tal es su relevancia que se regula con el conveniente detalle en el Tratado de Funcionamiento de la Unión Europea, así su artículo 88.1 del declara que: *"*La función de Europol es apoyar y reforzar la actuación de las autoridades policiales y de los demás servicios con funciones coercitivas de los Estados miembros, así como su colaboración mutua en la prevención de la delincuencia grave que afecte a dos o más Estados miembros, del terrorismo y de las formas de delincuencia que lesionen un interés común que sea objeto de una política de la Unión, así como en la lucha en contra de ellos.*"* A lo largo del punto dos[17] de este mismo artículo se especifican algunas de sus competencias, formulándolas con una formula abierta indicando así que no estamos ante un numerus clausus y se señala que el Parlamento Europeo y el Consejo son quienes, mediante reglamento, legislarán sobre todos los aspectos relativos a la policía europea. Para acabar, en el punto 3, se hace reflejar el necesario conocimiento y colaboración policial del concreto país miembro en cuyo territorio deba actuar la INTERPOL, delegando en los cuerpos de seguridad da este la ejecución de las eventuales medidas coercitivas.

[15] DE LA CORTE IBÁÑEZ. L, BLANCO NAVARRO. J.M., "seguridad nacional amenazas y respuesta" *LID editorial*, 2014, pág. 20

[16] http://europa.eu/abouteu/agencies/regulatory_agencies_bodies/pol_agencies/europol/index_es.htm fecha de consulta 13 de agosto de 2016

[17] Las competencias recogidas a titulo ejemplificativo, en el articulo 88.2 TFUE son las siguientes; "a) la recogida, almacenamiento, tratamiento, análisis e intercambio de la información, en particular la transmitida por las autoridades de los Estados miembros o de terceros países o terceras instancias; b) la coordinación, organización y realización de investigaciones y actividades operativas, llevadas a cabo conjuntamente con las autoridades competentes de los Estados miembros o en el marco de equipos conjuntos de investigación, en su caso en colaboración con Eurojust."

2. MARCO NORMATIVO DE LAS NUEVAS MEDIDAS DE INVESTIGACIÓN TECNOLOGICA CON ESPECIAL REFERENCIA AL USO DEL VIRUS: REFERENCIA A LA LEY 13/2015

El desarrollo no solo de las novedosas tecnologías o de los nuevos tipos de criminalidad que surgidos en los últimos años, sino también de los sistemas de investigación empleados por los cuerpos de seguridad han traído consigo la necesidad de regularizar la situación a fin de contar con un apoyo legal que proporcione seguridad jurídica y detalle los presupuestos de uso con el objeto de proteger los Derechos Fundamentales de los ciudadanos.

2.1. Marco normativo europeo

Antes de analizar el panorama legal de nuestro país es conveniente hacer mención a una esfera más amplia: la europea.

En este ámbito el texto legal más significativo en la materia es el Convenio Europeo sobre Ciberdelincuencia de Budapest[18]. Adoptado en noviembre de 2001, el convenio tiene dos principales objetivos. El primero se centra en tratar de armonizar determinados tipos delictivos[19]. El segundo da una serie de pautas o recomendaciones a los estados enfocadas a los medios de investigación de este tipo de delitos. En este sentido el artículo 15[20] hace hincapié en la necesidad de operar respetando en todo momento la ley y los derechos reconocidos en la misma y menciona como una de las salvaguardas la necesidad de supervisión judicial[21] cuando el procedimiento así lo requiera. Por su parte los artículos 20 y 21 del Convenio unificados en el título quinto de la sección segunda del capítulo segundo bajo el título *"*Obtención en tiempo real de datos informáticos*"* hacen referencia a los registros informáticos remotos, realizados mayoritariamente mediante el uso de softwares espías. Sin embargo se utiliza en la redacción del articulado una formula más abierta que permite la prolongación de la vigencia de las

[18] Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. BOE núm. 226, de 17 de septiembre de 2010, páginas 78847 a 78896

[19] Dentro del denominado Derecho penal Sustantivo (sección primera, capítulo segundo) se recogen los delitos que pretenden armonizarse, de este modo el título uno del texto recopila los delitos "contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos" el título dos los "Delitos informáticos" el título tres los " Delitos relacionados con el contenido" (centrándose en la pornografía infantil) el título cuatro, por último hace referencia a los " Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines"

[20] Artículo 15.1 del Convenio sobre la Ciberdelincuencia "Cada Parte se asegurará de que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades[…]"

[21] Artículo 15.2 del Convenio sobre la Ciberdelincuencia: "Cuando resulte procedente dada la naturaleza del procedimiento o del poder de que se trate, dichas condiciones incluirán, entre otros aspectos, la supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen la aplicación, y la limitación del ámbito de aplicación y de la duración del poder o del procedimiento de que se trate."

disposiciones. En concreto el Convenio señala que se deberán adoptar las medidas legislativas que sean pertinentes para dotar a la autoridad de poder para *"*obtener o a grabar mediante la aplicación de medios técnicos existentes en su territorio*"*.

A pesar de los evidentes avances que supone este Convenio el mismo presenta sin duda una importante deficiencia. Siendo la Unión Europea la máxima promotora de cooperación[22] entre estados extraña la no inclusión de disposiciones relativas al reconocimiento y la admisibilidad de la prueba entre los estados miembros de la Unión. Esta carencia se vio corregida ocho años más tarde ya que en 2009 se publicó por la Comisión Europea el llamado Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility (Libro Verde sobre la obtención de pruebas en materia penal en otro Estado miembro y sobre la garantía de su admisibilidad). Mediante este instrumento de cooperación se pretende *"*mantener y desarrollar un espacio de libertad, seguridad y justicia, en particular facilitando y acelerando la cooperación judicial en materia penal entre los Estados miembros*"* (como su propia introducción indica) mediante la realización de una serie de preguntas sobre la obtención y admisibilidad de pruebas a los estados miembros.

La Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de Agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, continua con esta labor persiguiendo la unificación de las legislaciones el plano de la lucha contra los delitos cibernéticos y el fomento de la cooperación ente estados.[23] Para garantizar dicha colaboración el artículo 13.1[24] ordena la creación y mantenimiento de un *"*punto de contacto nacional operativo*"* para el intercambio de información entre los estados y da un plazo máximo de ocho horas para que se indique si se atenderán y de qué forma las solicitudes de ayuda urgente al estado miembro emisor de esta. En

[22] Artículo 21.2 del Tratado de la Unión Europea "2. La Unión definirá y ejecutará políticas comunes y acciones y se esforzará por lograr un alto grado de cooperación en todos los ámbitos de las relaciones internacionales […]"

[23]La Directiva 2013/40/UE en su artículo 1, referente al objeto de la misma, señala: "La presente Directiva establece normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información. También tiene por objeto facilitar la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes"

[24] Artículo 13.1 de la Directiva 2013/40/UE: "A efectos del intercambio de información sobre las infracciones mencionadas en los artículos 3 a 8, los Estados miembros garantizarán que tienen un punto de contacto nacional operativo y harán uso de la red existente de puntos de contacto operativos disponibles veinticuatro horas al día, siete días a la semana. Los Estados miembros también se asegurarán de que cuentan con procedimientos para que, en caso de solicitud de ayuda urgente, la autoridad competente pueda indicar en un plazo máximo de ocho horas a partir de la recepción de la solicitud de ayuda si la misma será atendida, y la forma y el plazo aproximado en que lo será"

el artículo 13.2[25] se ordena a comunicar a la comisión cual es ese punto de contacto y en el artículo 13.3[26] se establece la obligación de mantener canales de comunicación adecuados disponibles. Se pretende también, en el artículo 9, la unificación de estándares mínimos en las sanciones para los delitos de esta naturaleza.

Tampoco podemos obviar en el ámbito europeo la Directiva 2011/93/UE relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil. Mediante este instrumento se pretende lograr, una vez más, la armonización entre los estados miembros de la Unión Europea en el plano de los de delitos de abuso sexual, explotación sexual y pornografía infantil[27]. Uno de sus objetivos principales es tratar de Establecer unos parámetros comunes para fijar un nivel mínimo en las penas impuestas a este tipo de delitos. Pero más allá de sus disposiciones en materia sancionadora también podemos encontrar preceptos relativos al derecho procesal. Así, En su articulado, se dispone que *"*Los Estados miembros adoptarán las medidas necesarias para garantizar que la investigación o el enjuiciamiento de las infracciones contempladas en los artículos 3 a 7*"*[28]. El texto faculta además a los estados miembros a "adoptar medidas para bloquear el acceso a las páginas web de Internet que contengan o difundan pornografía infantil a los usuarios de Internet en su territorio"[29].

2.2. Marco normativo español

Adentrándonos ya en el Derecho interno la ley encargada de regularizar y concretar los supuestos y requisitos de uso de este tipo de técnicas de investigación ha sido la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación

[25] Artículo 13.2 de la Directiva 2013/40/UE: "Los Estados miembros comunicarán a la Comisión su punto de contacto a que hace referencia el apartado 1. La Comisión transmitirá esta información a los demás Estados miembros y a los órganos y organismos especializados competentes de la Unión."

[26] Artículo 13.2 de la Directiva 2013/40/UE: " Los Estados miembros adoptarán las medidas necesarias para garantizar la disponibilidad de canales de información adecuados a fin de facilitar sin demora indebida a las autoridades nacionales competentes información relativa a las infracciones a que se refieren los artículos 3 a 6."

[27]La directiva 2011/93/UE en su artículo 2.c define del siguiente modo el concepto de pornografía infantil: i) todo material que represente de manera visual a un menor participando en una conducta sexualmente explícita real o simulada, ii) toda representación de los órganos sexuales de un menor con fines principalmente sexuales, iii) todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita real o simulada o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, o iv) imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales"

[28] Así viene reflejado en el artículo 15.1 de la Directiva 2011/93/UE. Dicho artículo nos remite s los delitos recogidos en los artículos 3, 4, 5, 6 y 7, siendo el 5 el relativo a "Infracciones relacionadas con la pornografía infantil" y el 6 al "Embaucamiento de menores con fines sexuales por medios tecnológicos"

[29] Articulo Artículo 25.2 de la Directiva 2011/93/UE "Medidas contra los sitios web de Internet que contengan o difundan pornografía infantil"

tecnológica. Se trata de una reforma muy necesaria como han hecho constar las voces expertas en la materia. Así por ejemplo FERNÁNDEZ TERUELO [30] señala que la legislación tanto penal como procesal con la que contamos en nuestro ordenamiento jurídico ha sido creada pesando en un *"*modelo de criminalidad física*"* por lo que, en consecuencia, no estaba preparada para afrontar las nuevas modalidades delictivas encuadrables en el cibercrimen. Por su parte BUENO DE MATA[31] afirma que mediante la reforma de la ley se pretende "dar cobertura legal a distintas diligencias de investigación que sirvan para investigar ciberdelitos de una manera garantista"

En sucesivos punto de este trabajo se expondrán de forma más detallada concretas disposiciones de la referida ley dando en este momento una visión más general de la misma. En primer lugar la propia ley en su preámbulo señala el objeto de su promulgación indicando que regularán "las medidas de investigación tecnológica en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales garantizados por la Constitución." Indica además que era preciso adoptar esta reforma con carácter "inmediato". Más adelante en el mismo preámbulo se reconoce la laguna normativa existente desde el amplísimo desarrollo de las nuevas tecnologías y los medios de comunicación hasta la promulgación de la ley y manifiesta su intención de equilibrar los derechos de los ciudadanos con la necesidad de luchar contra el cibercrimen, que había tenido que ser suplida mediante el desarrollo jurisprudencial[32]. La ley, por tanto, pretende regular en el campo de las diligencias de investigación tecnologías. Las medidas que recoge el texto legal con este fin se engloban desde el capítulo IV en adelante y son las siguientes: la interceptación de las comunicaciones telefónicas y telemáticas (capítulo V), la captación y grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos (capítulo VI), la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (capítulo VII), el registro de dispositivos de almacenamiento masivo de información (capítulo VIII) y registros remotos sobre equipos informáticos (capítulo IX).

[30]FERNÁNDEZ TERUELO, J., "Cibercrimen. Los delitos cometidos a través de internet", *Constitutio Criminalis Carolina*, 2007, pág. 13

[31]BUENO DE MATA. F., "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica" Nº 8627, *Diario La Ley*, 2015, Pág. 1

[32] Punto IV del preámbulo de la LO 13/2015: "Los flujos de información generados por los sistemas de comunicación telemática advierten de las posibilidades que se hallan al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos. Surge así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros. Por muy meritorio que haya sido el esfuerzo de jueces y tribunales para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática de nuestro sistema procesal"

2.3. Derecho comparado

La propia lo 13/2015 cuando hace referencia al registro remoto de equipos informáticos se refiere a ella en el punto IV del preámbulo como una "diligencia ya presente en buena parte de las legislaciones europeas". Más allá de nuestro país e incluso del derecho comunitario en otros estados también se ha podido observar cierta proliferación legislativa en la materia, como es lógico, dado que los avances en las nuevas tecnologías son un fenómeno global.

En reino Unido, ya en el año 2000 se empezó a regular en este ámbito mediante el Reglamento de la Ley de Poderes de Investigación del año 2000 (*Regulation of Investigatory Powers Act*). Sin embargo lo que el texto aparece no es la posibilidad de empelar sofwares de vigilancia si no de instalar dispositivos de captación de imagen y/o sonido y sea en el interior o en el exterior de vehículos, domicilios o lugares asimilados a fin de registrar lo ocurrido dentro de ellos. Los medios de seguridad, sin embargo, en los últimos años han tratado de subsumir las diligencias de investigación de acceso remoto a los dispositivos en esta legislación.

Por su parte la comunidad de países del Caribe conscientes de la necesidad de legislación en esta materia se han embarcado en un proyecto común junto con las Naciones Unidas[33] han creado el *"*Proyecto de Mejora de la Competitividad en el Caribe a través de la armonización de las políticas, legislaciones y procedimientos relacionados con las TIC*"*[34] con su creación se emiten una serie de recomendaciones legislativas relacionadas en gran parte con la prueba electrónica. Una de estas recomendaciones es que los cuerpos de seguridad puedan emplear como diligencia de investigación el uso de virus espía

En Australia los cuerpos de seguridad pueden instalar malewares y spywares en los equipos de los investigados desde la promulgación por el parlamento australiano de la Ley Surveillance Devices Bill de 2004 (acta número 152 de 15 de diciembre de 2004) la Organización Australiana de Seguridad e Inteligencia (Australian Security Intelligence Organisation) [35] en su acta ya prevé los servicios de inteligencia del país la posibilidad del uso de softwares que permitan el acceso remoto a dispositivos informáticos.

[33] Más concretamente con un organismo especializado y dependiente de las Naciones Unidas La Unión Internacional de Telecomunicaciones (ITU)
[34] www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/ fecha de consulta 16 de agosto de 2016
[35] The Australian Security Intelligence Organisation (ASIO) se define a sí misma como un servicio de seguridad estatal cuyo principal interés es proteger la seguridad de Australia y defender los intereses del país y de sus ciudadanos frente al espionaje, al sabotaje, a la violencia por motivos políticos, a la promoción de la violencia comunitaria, a los ataques contra el sistema de defensa de Australia, a los actos de interferencia extranjera o las serias amenazas a la integridad territorial y la frontera de Australia. https://www.asio.gov.au/what-we-do.html

En Alemania fue más complicada esta implantación pues su Tribunal Supremo había declarado que no existía norma legal en la que poder amparar el uso del acceso remoto como diligencia de investigación. Fue necesario un cambio de planteamiento por parte del Tribunal Constitucional Alemán (Bundesverfassungsgericht) [36]y el reconocimiento por parte de este de un nuevo derecho fundamental (el "Derecho Fundamental a la garantía de la confidencialidad e integridad de los equipos informáticos") para reformar la Bundeskriminalamt (Ley del Servicio Federal de Investigación Criminal) e incluir esta posibilidad.

[36] El reconocimiento del nuevo derecho se dio mediante la sentencia de 27 de febrero de 2008 BVerfG, 1 BvR 370/07 de 27.2.2008 en la cual se debatía sobre el alcance que debe tener la protección de datos en el marco actual de las nuevas tecnologías. La sentencia se da en el marco del planteamiento de un recurso interpuesto contra la reforma de la ley de los servicios de inteligencia del Estado de Renania del Norte Westfalia mediante la cual se permitía el uso de software espía a los cuerpos de servicios de inteligencia. Aquella reforma fue declarada inconstitucional sin embargo se dieron las bases acerca de los requisitos que debe cumplir una ley para recoger tales practicas sin atentar contra este nuevo Derecho Fundamental reconocido

3. EL USO DE SPYWARE Y MALEWARE COMO DILIGENCIA DE INVESTIGACIÓN

3.1. Conceptualización

Antes de entrar a analizar esta concreta medida de investigación policial debemos tener claro un concepto más amplio, que no puede ser otro que el de diligencia de investigación policial. Nos encontramos ante una de estas medidas cuando se lleva a cabo un acto de instrucción dirigido a investigar la comisión de un determinado delito. Dependiendo del tipo de delito cometido y de las medidas que sea necesario adoptar para u investigación se recurrirá a un tipo de medida o a otra dándolo lugar a sí a tipos específicos de diligencias policiales. En ocasiones, debido a las características propias de la información contenida en aparatos tecnológicos, es difícil acceder a la prueba. Esto se debe, entre otros motivos, a la volatilidad de los datos, las variadas posibilidades de ocultación, los sistemas de protección de datos, el gran volumen de información existente… Por este motivo la actuación policial muchas veces se ve obligada efectuar operaciones de *Hacking*[37] como una posibilidad de recabar la evidencia necesaria ante determinados tipos delictivos, posibilidad que la propia LO 13/2015 recoge cuando emplea la expresión *"*Podrá […] por cualquier medio técnico*"*[38] Estas técnicas de hackeo pueden llevarse a cabo sobre el equipo informático que pretende intervenirse cuando este ya se encuentra en poder los cuerpos de seguridad del estado pero también puede que la aprehensión del dispositivo no se haya llevado a cabo. En este caso el acceso al mismo será remoto y el hackeo se llevado a cabo de forma telemática. La necesidad de acceder "a distancia" a los datos de un investigado puede venir motivada por muchos factores, ORTRIZ PRADILLO[39] menciona alguno de ellos, como por ejemplo la imposibilidad de acceder al dispositivo de forma física por no conocer su ubicación, necesitar información que se encuentre almacenada en la memoria RAM (y por tanto que desaparecerá al apagar el ordenador) o para evitar que ante una inminente entrada en su domicilio el investigado ejecute algún software de borrado de datos eliminando las evidencias de su actividad delictiva.

[37] El hacking, según el glosario de argot hacker Jargon File, creado por Eric S. Raymond, consiste en acceder forzosamente a un sistema informático así como su alteración o interrupción.

[38] Así aparece en el artículo 588 quinquies a referente a la Captación de imágenes en lugares o espacios públicos o en el artículo 588 ter l relativo a Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes.

[39] ORTIZ PRADILLO, J.C., "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica" en "El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito", edición nº 1, *Editorial LA LEY,* 2012. Pág. 3

Antes de adentrarnos en una explicación más detallada de estas técnicas conviene hacer referencia a que no son el único método de acceso remoto a los datos contenidos en un determinado positivo. La ley prevé otra opción que permitiría conocer los sitios web visitados así como el flujo de datos enviados y recibidos desde un equipo informático. Estamos hablando de la intervención de la línea de datos o del ADSL. Con el objeto de aportar una definición más técnica citamos a VELASCO NUÑEZ,[40] autor que define esta diligencia del siguiente modo: "Intervención de la información que fluye de entrada y salida de un concreto ordenador mediante el sistema de monitorizar o duplicar en tiempo real o posterior y en forma local o remota, toda la actividad dinámica de sus usuarios".

Para el uso de esta medida es necesaria la colaboración de proveedor de datos, lo que, por lo general, supone una complicación añadida respecto del uso de virus espías como veremos más adelante. Sin embargo existen ocasiones en las que incluso recurriendo al uso de virus espías podría precisarse la colaboración de terceros. La problemática es muy relevante en este tema por lo que conviene hacer un paréntesis para debernos en ella La LO 13/2015 prevé en su articulado la necesaria ayuda que deben prestar terceras personas ante diligencias de registros remotos sobre equipos informáticos. El Artículo 588 septies b., bajo el enunciado: "Deber de colaboración" regula esta circunstancia en su apartado primero: "Los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro están obligados a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización." La ley, en el apartado dos del citado artículo, extiende la obligación de colaborar no solo a los proveedores de datos si no a "cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo". Matiza la ley que el término "cualquier persona" no se extiende al propio investigado (respetando así el Derecho Fundamental [41] a no declarar contra sí mismo) ni a otras personas respecto a las que exista una dispensa de declarar, esto es: las relacionadas por parentesco[42] conforme a lo dispuesto en la ley y aquellas que no puedan

[40] VELASCO NUÑEZ, E., "ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal" Nº 82, *Editorial LA LEY*, 2011, Pág. 2.

[41] Articulo 24. 2 de la Constitución Española: "Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia."

[42] Artículo 416.1 de la Ley de Enjuiciamiento Criminal: "Están dispensados de la obligación de declarar: Los parientes del procesado en líneas directa ascendente y descendente, su cónyuge o persona unida por relación de hecho análoga a la matrimonial, sus hermanos consanguíneos o uterinos y los colaterales consanguíneos hasta el segundo grado civil, así como los parientes a que se refiere el número 3 del artículo 261."

hacerlo en virtud del secreto profesional[43]. Además la ley impone un deber estrictamente relacionado con el de colaboración: el de guardar secreto [44] a expensas del buen fin de la investigación, del tal modo que si no se respetaran estos dos deberes, los terceros implicados, podrían incurrir en responsabilidades[45] (materializadas en forma de delito de desobediencia[46]).

Dada la exagerada amplitud de este precepto que permite literalmente la participación obligada de "cualquier persona" en unas diligencias de investigación policiales se han levantados voces detractoras del mismo. Así por ejemplo BUENO DE MATA [47] vincula dos efectos negativos a este tipo de redacción generalista e indeterminada. Por un lado considera que se está banalizando acerca de las complicadas tareas que asumen los agentes de policía en los siguientes términos "se desvalora o se reconoce como insuficiente la capacitación técnica de la policía judicial en términos de investigación policial, cuando existen unidades concretas con miembros con años de especialización que han sido formados para tal fin y están en constante reciclaje y capacitación, por lo que a nivel publicitario y de imagen exterior no creemos que nos haga ningún bien" Por otro lado se cuestiona la problemática que supondría englobar en este masa indeterminada de personas a "hackers que actúen sin fines éticos e incluso criminales" situación que perfectamente podría darse teniendo en cuanta que, como acabamos de ver, la ley solo excluye al propio investigado y a individuos con dispensa del deber de declarar por motivos de parentesco o secreto profesional. Cabe señalar que esta injerencia solo se presenta en una magnitud tan grande al hablar de registro remoto de equipos informáticos. Si acudimos al párrafo primero del artículo 588 sexies c.5[48], referente a Registro de dispositivos de almacenamiento masivo de información, comprobamos que se faculta a la autoridad ordenar a cualquier persona que "facilite la información que resulte necesaria". Se habla únicamente de suministrar información mientras que cuando hablamos de registro remoto el deber de colaboración implica toda aquella que resulte necesaria para "práctica de la medida y el acceso al sistema" así como "la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización". Tal diferenciación ha sorprendido a algunos autores que

[43] Específica la LO 13/2015 que la dispensa se aplicará respecto de aquellas personas mencionadas en el artículo 416.2 de la Ley de Enjuiciamiento Criminal, a saber: "El Abogado del procesado respecto a los hechos que éste le hubiese confiado en su calidad de defensor."
[44] Artículo 588 septies b. 3 de la LO 13/2015: "Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades."
[45] Artículo 588 septies b. 4 de la LO 13/2015: "Los sujetos mencionados en los apartados 1 y 2 de este artículo quedarán sujetos a la responsabilidad regulada en el apartado 3 del artículo 588 ter e."
[46]artículo 588 ter e., apartado 3, de la LO 13/2015: "Los sujetos obligados que incumplieren los anteriores deberes podrán incurrir en delito de desobediencia"
[47] BUENO DE MATA F., "Comentarios y reflexiones": …,cit.,p. 6
[48]Artículo 588 sexies c.5 de la LO13/2015 "Las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia."

entienden que la complejidad de acceso a los datos será misma cuando estemos ante un registro remoto que cuando los agentes de la autoridad tengan en sus dependencias físicamente el dispositivo del que pretende obtenerse la información. RODRÍGUEZ LAINZ[49] apunta que la diferenciación posiblemente se deba a que "el legislador posiblemente no tuviera clara la solución definitiva al problema; y que la opción final pudiera ser más consecuencia de una no muy reflexiva redacción de ambos supuestos, que fruto de una decidida determinación por imponer un régimen más amplio de colaboración en los supuestos de registro remoto" a esta conclusión llega tras examinar el Borrador de Anteproyecto de Código Procesal Penal de diciembre de 2012 por un lado y el borrador de anteproyecto de la LO 13/2015. En el primero se daba más amplitud al deber de colaboración en los registros remotos y en el segundo al registro físico. RODRÍGUEZ LAINZ considera que esta disparidad no debería tener relevancia práctica puesto que una interpretación sistemática de la norma nos llevaría a extender el deber de colaboración "reforzado" del artículo 588 septies B al 588 sexies c.5. En mi opinión efectuar una interpretación de estas características sería dar mayor ámbito de aplicación y trascendencia a una previsión legal demasiado amplia. A mi juicio el precepto 588 septies B requiere corrección puesto que obligar a cualquier persona a prestar deber de colaboración, además de ser un mandando de una indeterminación reviste consecuencias perniciosas como ya subrayaba BUENO DE MATA. Ampliar sus efectos a otro tipo de diligencias de investigación supondría, por lo tanto empeorar la regulación.

Volviendo sobre la intervención de la línea de datos o del ADSL, otro punto en contra de esta medida en comparación al uso de maleware y spyware es que el volumen de indicios obtenidos es considerablemente menor en este caso. Eso debe a que mientras los virus espías pueden acceder a toda la información contenida en un equipo la intervención de los datos solo permite obtener la información que sale a la red[50] pero no aquella almacenada en la memoria interna. Es por estos motivos que suele emplearse más está diligencia no para un espionaje continuado si no para mementos puntuales, como por ejemplo cuando el presunto delincuente se conecte a la red desde un equipo del que no es titular. A titulo ejemplificativo, hace unos años una de las medidas más empleadas en EEUU por el FBI, en este campo y que se basa en esta técnica es el llamado "sistema carnívoro" también conocido como "DCS1000". Se instalaba en los equipos de los proveedores de internet y mediante su uso se extraía el flujo comunicativo

[49]RODRÍGUEZ LAINZ, J.L., "¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?", Nº 8729, Editorial LA LEY, 2016, Pág. 7

[50] VELASCO NUÑEZ, E., "ADSL Y TROYANOS":…cit., p. 3. El autor señala que los datos que pueden obtenerse mediante esta diligencia son: "datos de entrada y salida, correos-e, mensajes y archivos que adjunten, VoIP, fax, video IP, escucha en tiempo real, contraseñas (*passwords*) y procesamiento de web mails, P2P, intercambios y redes de intercambio, Chats, mensajería instantánea, grupos de noticias y páginas web consultadas en Internet, si está descargando información y desde dónde"

llevado a cabo mediante la red. Por su parte las técnicas de hackeo se llevan a cabo en números ocasiones mediante el uso de virus informáticos. Los virus son programas informáticos capaces de adentrarse en un sistema y causar perjuicios en él, es por esto que los virus se engloban dentro de la categoría del llamado maleware. Estamos hablando de operaciones de monitorización de los datos dispuestas para la búsqueda de información encaminada por un lado, a la averiguación de los hechos delictivos y de los participes en los mismos, y por otro lado, a la obtención de pruebas en sentido estricto como elementos validos para demostrar la comisión y autoría de un hecho delictivo.

AMÉRIGO SÁNCHEZ[51] define el *maleware* como "cualquier programa informático capaz de ocasionar un daño, ya no sólo al sistema informático en el que se ejecuta, sino al propio usuario, como, por ejemplo, mediante la obtención de sus datos bancarios, de información personal, de archivos íntimos, etc. El malware es un concepto más amplio que el virus informático; abarca también programas como los troyanos, el *spyware*, los *keyloggers*, etc." Es decir, los *malewares*[52] están diseñados para causar efectos perniciosos de la más diversa índole en equipos informáticos que inevitablemente, acaban afectando al usuario del equipo por la gran cantidad de información personal que esta clase de dispositivos contiene. Esto lo logran aprovechando los defectos o vulnerabilidades existentes en los softwares instalados en los equipos.

Por su parte los *spyware* (o virus espía) como su propio nombre indica son una clase de virus (y, por tanto, un subtipo de *maleware*) capaces de obtener información copiarla o clonarla y transmitirla a un tercero sin el consentimiento (ni conocimiento) del titular de los datos recabados. En otras palabras un spyware es un *maleware* cuyo concreto efecto nocivo es su capacidad de copiar y trasmitir la información existente en el equipo en el que se aloja. Es suficiente con una lectura de esta definición para darnos cuenta de la gran cantidad de información que puede obtenerse con una medida de estas características. Hoy en día los ciudadanos utilizan los distintos dispositivos electrónicos para guardar un porcentaje amplísimo de sus datos. En un ordenador, por ejemplo, las personas guardan sus archivos audiovisuales, datos bancarios, expedientes, documentos oficiales, registros de las comunicaciones mantenidas con otros usuarios… en definitiva nos encontramos una ante un tipo de diligencia de investigación tan útil como invasiva de la privacidad. Por su propia naturaleza, inevitablemente el uso de este tipo de recursos va a encontrarse en constante colisión con los derechos fundamentales los investigados, como veremos más adelante, motivo por el cual será preciso

[51] AMÉRIGO SÁNCHEZ J.L., "El régimen jurídico del malware según la Ley de Propiedad Intelectual" Nº 8436, *Diario La Ley*, 2014, Pág.4

[52] Maleware es un nombre que se deriva de la expresión inglesa malicious software o software malicioso. Este tipo de software recibe, en la misma línea otro tipo de nombres como por ejemplo código maligno, badware, o software malintencionado

extremar las cautelas referentes a su uso. Su uso por tanto debe ser reservado para situaciones en las que sea verdaderamente necesario por no existir otra medida menos invasiva de la intimidad de las personas para el supuesto específica ante el que nos encontremos. Además su aplicación no debe ser indiscriminada si no limitarse únicamente a recabar aquella información que vaya a ser útil para la investigación. Esta tarea puede verse facilitada si se emplean como apoyo complementario a la media *softwares* buscadores de palabras clave. De este modo se lograrían seleccionar solo aquellos datos relevantes para la instrucción evitando injerencias en los que no lo sean. El efecto beneficios de estas técnicas es doble, no solo supone una vulneración menor de derechos si no que facilita y agiliza el trabajo de los investigadores.

3.2. Tipos de virus usados y función de cada uno de ellos

Antes de seguir desarrollando este punto, y con él las técnicas de acceso remoto a equipos informáticos, debemos aclarar que la ley no recoge lista tipológica alguna que determine qué tipo de *softwares* informáticos van a poder ser utilizados. Esto, nuevamente, supone inseguridad jurídica para el ciudadano ya que la consecuencia directa de esta deficiencia es no poder conocer tampoco los límites a los procesos informáticos que se permiten. De este modo podría utilizarse un virus espía cuyas facultades sean muy amplías y quizás demasiado invasivas. Por tanto y ante la imposibilidad de hablar de la tipología recogida en la ley, por su inexistencia, nos referiremos a alguno de los softwares más significativos en la práctica. Todos esos programas pueden tienen en común que "abren la puerta" a intromisiones externas. Por este motivo pueden ser englobados bajo la categoría de programas *blackdoor*[53] o programas de puerta trasera y vendrían a suponer un acceso a un equipo informático camuflado de modo que el investigado no tendría conocimiento acerca de él.

Por medio de los procesos informáticos llevados a cabo por estos programas se consigue el llamado *remote search* o registro remoto de equipos. ORTIZ PRADILLO[54] define estos procesos como a "la técnica consistente en el acceso y registro de los equipos electrónicos e informáticos del sujeto investigado, de forma remota y telemática, mediante la previa instalación en el mismo del software necesario -los denominados «programas troyanos»- que permita a las autoridades responsables de la investigación, escanear su disco duro y demás

[53] En sitios web especializados en informática, como por ejemplo ZonaVirus se define los blackdoor del siguiente modo: "Las puertas traseras (backdoors) son programas que permiten acceso prácticamente ilimitado a un equipo de forma remota […] se instalan en el sistema sin necesidad de la intervención del usuario y una vez instalados, no se pueden visualizar estas aplicaciones en la lista de tareas en la mayoría de los casos. Consecuentemente un backdoor puede supervisar casi todo proceso en las computadoras afectadas, desinstalar programas, descargar virus en la PC remota, borrar información, entre otras muchas cosas más" http://www.zonavirus.com/articulos/puertas-traseras-o-backdoors.asp fecha de consulta 12 de agosto de 2016

[54] ORTIZ PRADILLO, J.C., "El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito" ,nº 1, Editorial LA LEY, 2012, Pág. 5

unidades de almacenamiento y remitir de una manera remota y automatizada el contenido del mismo a otro equipo informático (el de la autoridad responsable de la investigación).”

Precisamente es el llamado virus troyano, caballo de Troya o *Trojan horse* uno de los instrumentos más utilizados por cuerpos de investigación debido a las importantes utilidades que supone su uso. Cabe señalar en primer lugar que no todos los virus troyanos son virus espías, algunos virus troyanos están diseñados para causar otro tipo de efectos como destruir información del equipo. Por este motivo aunque en el lenguaje coloquial virus troyano se emplee como sinónimo se *spyware* no tiene por qué ser así. VELASCO NUÑEZ al hablar de los troyanos espías explica que esta técnica consiste en: “la entrada subrepticia de un programa en el ordenador de un sospechoso, pretende adquirir pruebas y vigilar la actividad de éste, consiguiendo sin su conocimiento, pero con autorización judicial, los datos que aquel almacena en su disco duro o en la memoria del PC, así como toda la actividad comunicativa que no sale a la Red […] además del tráfico de entrada y salida de sus telecomunicaciones y de las páginas web que visita”[55]. Como puede extraerse de esta definición las principales ventajas que este tipo de virus proporciona son: la posibilidad de obtener tanto la información almacenada en el equipo informático como aquella que se produce *on-line* (lo que supone un gran incremento del volumen de datos), el acceso remoto a la fuente de prueba (no será preciso por lo tanto un registro presencial en el domicilio) la discrecionalidad[56] (ya que el investigado no tendrá constancia de que el *software* ha sido instalado en su ordenador), la inmediatez en la recogida de material probatorio (de forma instantánea los datos quedan transferidos para su posterior estudio por parte de los agentes expertos en la materia, el cual también será más rápido, sencillo y eficaz debido a la automatización y sistematización conseguida mediante la configuración concreta del virus, permitiendo así la selección de los datos que revistan mayor utilidad). En relación a esto existen a su vez programas informáticos que adheridos o combinados con los virus espía permiten una rápida localización de “palabras clave”. Esto supone aumentar de forma drástica la rapidez de las búsquedas, tarea que resulta imprescindible al trabajar con un volumen de datos tan grande.

Otra de las técnicas empleadas para la investigación de delitos mediante diligencias tecnologías es el uso de *keylogger*, o en castellano, lector de teclados. VELASCO NÚÑEZ[57]

[55] VELASCO NUÑEZ, E., “ADSL Y TROYANOS”:…cit., p. 4.
[56] Una de sus características más relevantes es precisamente la discrecionalidad en su instalación de tal modo que la misma resulta “invisible” para el usuario del equipo. Este es el motivo por el cual los virus troyanos reciben su nombre. Su origen etimológico se debe por tanto a la historia del caballo de Troya, famoso pasaje de la mitología griega en el que se cuenta como los soldados griegos consiguieron entrar en la ciudad de Troya escondidos en un enorme caballo de madera.
[57] VELASCO NÚÑEZ.E, “Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías” número 4, *Revista de Jurisprudencia,* 2011. Pág.2

explica que este procedimiento se emplea "ante la necesidad de captar actuaciones interactivas no monitorizables en el investigado (especialmente su clave y contraseña) pudiera instalarse con autorización judicial como complemento técnico de lo que jurídicamente es la interceptación de la información de interés para la investigación en los ordenadores." Por tanto se trata de un programa capaz de registrar las pulsaciones del teclado y de este modo obtener información, contraseñas y todo tipo de claves.

A pesar de las innumerables ventajas de este tipo de medidas las mismas también revisten ciertos inconvenientes. El primero y el principal de ellos es que, como todos los *softwares* espías, pueden ser detectados por los antivirus y una vez localizados el investigado puede eliminarlos de su equipo con relativa facilidad. Una posible solución a este problema sería contar con la ayuda de los técnicos encargados de proveer antivirus y pactar con ellos que no desactiven aquellos empleados por los cuerpos de seguridad, pero esta solución tampoco estaría exenta de inconvenientes ya que estaría incluyendo nuevamente intermediarios a los cuales se les estaría obligando a ir en contra de sus propios intereses.

En la práctica existen dos métodos de alojar el virus en el equipo que pretenda "espiarse". Mediante el primero de ellos se instalan ciertos enlaces portadores del virus en páginas web cuyo contenido sea sospechoso de atraer a determinados delincuentes. De este modo el internauta se auto instala el virus al *clickar* en el botón de descarga. Las vulnerabilidades básicas de este método son por un lado la imposibilidad de individualizar a un sospechoso en particular, ya que afectaran a todo el que visite esas páginas y por otro el hecho de emplear sitios web de titularidad ajena puede acarrear que los enlaces sean más fácilmente detectados. El segundo método elimina a las páginas webs como intermediarias en la operación. Los investigadores envían directamente correo electrónico a los sospechosos conteniendo los enlaces portadores del troyano. Aquí donde el acceso remoto a los datos se apoya en otra diligencia de investigación policial reformada por la LO 13/2015 para otorgarle nuevas competencias: el agente encubierto[58] informático. En primer lugar debemos señalar que el agente encubierto informático es un policía que bajo una identidad supuesta realiza sus investigaciones infiltrándose entre los presuntos delincuentes, en este caso con la particularidad de que se infiltra en el ámbito de las nuevas tecnologías y las comunicaciones electrónicas. Dicha figura se regula en el artículo 282 bis de la Lecrim a cuya redacción la reforma ha añadido los puntos 6

[58] La figura del agente encubierto como medio de investigación procesal nació de la mano de la LO 5/1999 de 13 de enero, aunque en la práctica ya se venía usando en materia de seguridad. La Sentencia del Tribunal Supremo 1140/2010 de 29 de diciembre define al agente encubierto como: "el policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la Ley y bajo el control del Juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación o estos sean manifiestamente insuficientes, para su descubrimiento y permite recabar información sobre su estructura y modus operando, así como obtener pruebas sobre la ejecución de hechos delictivos"

y 7. El punto relacionado con el uso de *spywares* es el 6, párrafo dos, en el cual se dispone lo siguiente: "El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos." Esta disposición implica dos tipos diferentes de actuaciones con relevancia en el registro remoto de equipos.

La primer tipo supone que el agente está facultado para difundir material ilícito con el objeto de infiltrarse en una determinada red criminal. De este modo el policía encubierto estaría trasmitiendo archivos que posteriormente podrían ser localizados por los *softwares* espías. Por este motivo es importante dejar constancia en un fichero de qué material es el que se está enviando a los equipos de los sospechosos. Para ello se utilizaría una técnica comparativa de códigos hash, que explicaremos más adelante en el punto relativo a la cadena de custodia de la prueba. Cabe señalar, con respecto a esta ampliación de competencias, que algunos autores han señalado ya los riesgos implícitos en esta práctica. Así por ejemplo RUBIO ALAMILLO[59] asevera que: "es necesario incidir también en el hecho indiscutible que supone como incitación a cometer una actividad delictiva el envío de un fichero ilícito a un ciudadano, toda vez que, un delincuente real, podría diseminar estos archivos por la red sin control, siendo encontrados en intervenciones domiciliarias por la Policía Judicial y sin saber si realmente dichos ficheros fueron enviados por la Policía como señuelo, o por delincuentes reales que tomaron esos ficheros policiales y luego los diseminaron como parte de su actividad criminal."

El segundo tipo englobaría los supuestos de envío de virus espías. En este caso sería el agente encubierto informático el que enviaría, por ejemplo al correo electrónico del investigado, los link de descarga camuflados, que realmente contiene un software espía.

El desarrollo de las nuevas tecnologías y su uso para la comisión de delitos ha traído aparejada la necesidad de innovar en las técnicas de investigación y de adaptar estas a los avances electrónicos. De este modo, en ocasiones, el uso de virus espía se convierte en la única manera de investigar un delito. Es evidente que en un estado constitucional protector y garante de los derechos de los ciudadanos una técnica de estas características debe estar prevista y regulada en la legislación. Aunque la LO 13/2015 se ha encargado de regular estas cuestiones a mi juicio la regulación existente en la misma es insuficiente. Las lagunas en su redacción levantan interrogantes que a día de hoy no han podido resolverse. Una de las mayores incertidumbres que arroja es precisamente con respecto al tipo de virus espía que pueden usarse en las diligencias de investigación policiales. No se trata de una cuestión irrelevante ya que

[59] La informática en la reforma de la Ley de Enjuiciamiento Criminal Javier RUBIO ALAMILLO Diario La Ley, Nº 8662, Sección Tribuna, 10 de Diciembre de 2015, Ref. D-463, Editorial LA LEY. PAG 5.

conocer el tipo de virus permitidos implica conocer el alcance de la intromisión en los equipos informáticos y al mismo tiempo y sentido contrario, impide intrusiones de una magnitud mayor a la regulada en la ley. De este modo aunque la entrada en vigor de la ley ha supuesto un logro jurídico en mi opinión es necesaria una ampliación de la misma que regule estas cuestiones. Dicha ampliación debería ser capaz de encontrar un equilibrio entre aportar mayor seguridad jurídica y no ser un texto legal demasiado cerrado que con el paso del tiempo y los avances de la tecnología pueda quedarse desfasado o carente de utilidad por obsolescencia de sus términos.

Uno de los países donde mejor podemos ver reflejada esta realidad es Estados Unidos. Allí los cuerpos de seguridad han tenido la oportunidad de trabajar con varios *softwares* espías cuya tipología explicaremos brevemente a continuación. El virus carnívoro, cuyo nombre oficial es DCS1000[60] es uno de los más conocidos. Fue empleado durante varios años empezando su andadura en el año 1997. Este sistema se instalaba en la red del proveedor de datos y por medio de un programa sniffer [61] realizaba un seguimiento y registro de las comunicaciones efectuadas a través de ellos de este modo se recogen todos los e-mails enviados así como otras comunicaciones efectuadas por medio de chats o foros y demás aplicaciones de mensajería instantánea, y se consigue un registro de todas las webs visitadas.

Poco después comenzó a usarse en este mismo país un nuevo software conocido como Linterna Mágica"(*Magic Lantern*). La ventaja principal con respecto al virus carnívoro era que se instalaba directamente en el equipo informático investigado y no en la red el proveedor de datos. Linterna mágica es un ejemplo de la técnica *keylogger* puesto que se trata de un troyano que mediante el lector de teclados se emplea para la obtención contraseñas de los investigados.

Uno de los subtipos de virus troyanos más empleado en la actualidad en Estados Unidos para la investigación policial llevada a cabo por el FBI es el CIPAV (Computer and Internet Protocol Address Verifier) aunque su manera de usarlo haya levantado especulaciones y voces disonantes[62]. Este tipo de software, como su propio nombre indica, (en español "verificador de IP") se limita a hacer un registro de las IP visitadas por el usuario del ordenador sin embargo no se obtiene contenido alguno acerca de las comunicaciones realizadas.

---

[60] El nombre viene de las siglas en ingles de Digital Collection System, lo cual se traduce por Sistema de Recolección Digita que en español vendría a significar Sistema de Recolección Digital.

[61] Un Sniffer es un software encargado de registrar la actividad en línea llevada a cabo por un ordenador. Recibe este nombre porque absorbe todos los datos que circulan por una determinada red

[62] En el año 2015 la AP (The Associated Press o asociación de periodistas) interpuso uno demanda contra el FBI acusándole de haber infiltrado a uno de sus agentes en sus oficinas de trabajo. Este haciéndose pasar por periodista habría redactado una noticia falsa que habría enviado a un adolescente sospecho de enviar avisos falsos de bomba con el objeto de instalar en su ordenador el software CIPAV. http://eleconomista.com.mx/internacional/2015/08/27/ap-demanda-fbi-hacerse-pasar-agencia fecha de consulta 15 de agosto de 2016

3.3. Tipo penal y ámbito de aplicación

La reforma de la ley 13/2015 cumpliendo con su cometido de regular las novedades en materia de investigación mediante la utilización de las nuevas tecnologías ha introducido en su articulado la delimitación de los tipos delictivos en los que puede emplearse los virus espías. Los mismos se recogen en el artículo 588 septies a.1 de Ley de Enjuiciamiento Criminal el cual enumera cinco tipos delictivos generales, a saber: "a) Delitos cometidos en el seno de organizaciones criminales. b) Delitos de terrorismo. c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente. d) Delitos contra la Constitución, de traición y relativos a la defensa nacional. e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación." Con el objeto de ahondar un poco más en los tipos penales para los que se prevé el uso de este tipo de diligencias de investigación daremos una breve conceptualización.

Al hablar de delitos cometidos en el seno de una organización criminal estamos haciendo referencia al tipo regulado en el párrafo segundo del punto primero del artículo 570 bis del Código Penal. En él se dispone que: "A los efectos de este Código se entiende por organización criminal la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos." Por su parte GONZÁLEZ RUS[63] las define al crimen organizado como: "el resultado de una unión de una pluralidad de personas, dotada de una entidad independiente de sus miembros con un esbozo de organización, jerarquía y división del trabajo, y dirigido al logro de un fin delictivo"

Con respecto a los delitos de terrorismo se configuran en la sección primera del capítulo VII de nuestro Código Penal en concreto en el artículo 571 el cual dispone que "A los efectos de este Código se considerarán organizaciones o grupos terroristas aquellas agrupaciones que, reuniendo las características respectivamente establecidas en el párrafo segundo del apartado 1 del artículo 570 bis y en el párrafo segundo del apartado 1 del artículo 570 ter, tengan por finalidad o por objeto la comisión de alguno de los delitos tipificados en la sección siguiente." El referido artículo 570 bis, recientemente mencionado, define las organizaciones criminales. El 570 ter define a los grupos criminales del siguiente modo: "A los efectos de este Código se entiende por grupo criminal la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal definida en el artículo anterior, tenga por finalidad o por objeto la perpetración concertada de delitos." Por último cuando el artículo hace referencia a los "delitos tipificados en la sección siguiente" se está refiriendo a los

[63]GONZÁLEZ RUS, J.J., "La criminalidad organizada en el Código Penal español. Propuesta de reforma". núm. 30, *Anales de Derecho*, 2012, pág. 25.

comprendidos entre el propio artículo 571 y el 580. En ellos se contienen pluralidad de conductas sin embargo las más reseñables se encuentran en el artículo 573, en concreto en el punto 1: " Se considerarán delito de terrorismo la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexuales, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, contra la Corona, de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos, previstos en el presente Código, y el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías" en el artículo 574.1[64], referido a la tenencia y tráfico de armas y municiones. La relación entre terrorismo y nuevas tecnologías es cada vez más estrecha de ahí la importancia de desplegar métodos de investigación basados también en estos avances. VELASCO NUÑEZ [65] señala que esta relación se basa principalmente en dos factores. El primero es la necesidad que tiene todo grupo u organización de personas con un fin común de mantener comunicaciones constantes. El segundo es utilizar las nuevas tecnologías como el instrumento de ataque. Bien para facilitar la comisión de delitos convencionales (uso de *softwares* para conseguir claves y así facilitar la realización del delito de estafa) o bien delitos estrictamente informáticos (como el uso de virus espías para la obtención de información).

Los delitos cometidos contra menores o personas con capacidad modificada judicialmente encuentran su razón de ser dentro de la relación en el artículo 588 septies de la Ley de Enjuiciamiento Criminal por proteger a sujetos pasivos especialmente vulnerables. No es la primera vez que el legislador penal establece esta especialidad. Es recurrente encontrar una fórmula similar para otros delitos, como en el caso de los delitos contra la vida y la integridad física o moral[66], de la violencia de género[67] o de de exhibicionismo y provocación sexual[68]. Existen además delitos de específica comisión en el ámbito de internet y cuyo objeto pasivo son los menores. Por la gran importancia que revisten estos delitos nos detendremos a hablar de alguno de los más relevantes. Así podemos encontrar como delitos tipificados en nuestro Código Penal el *child grooming* y el *sexting*. El artículo 183 Bis del Código Penal mediante su

[64] Artículo 574.1 del Código Penal: "1. El depósito de armas o municiones, la tenencia o depósito de sustancias o aparatos explosivos, inflamables, incendiarios o asfixiantes, o de sus componentes, así como su fabricación, tráfico, transporte o suministro de cualquier forma, y la mera colocación o empleo de tales sustancias o de los medios o artificios adecuados"

[65] VELASCO NÚÑEZ E., "Delitos informáticos realizados en actuación organizada", Nº 7743, *Diario La Ley*, 2011, Págs. 1 y 2.

[66] En el aparado segundo del artículo 57 del código penal se recoge una de estas especialidades con respecto a menores y personas con la capacidad judicialmente modificada y en aparatado primero del citado artículo se indican los delitos para los que se aplicará dicha especialidad siendo estos: "homicidio, aborto, lesiones, contra la libertad, de torturas y contra la integridad moral, trata de seres humanos, contra la libertad e indemnidad sexuales, la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, el honor, el patrimonio y el orden socioeconómico"

[67] Artículo 153.3 del Código Penal, referido al 153.1

[68] Artículo 185 del Código Penal: "El que ejecutare o hiciere ejecutar a otra persona actos de exhibición obscena ante menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses."

redacción indica que penalizarán las siguiente conductas: "1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, […]. Este primer apartado del articulo esta penalizando las conductas de *child grooming*. Las nuevas tecnologías, y en especial aquellas que facilitan las comunicaciones y las dotan de anonimato ha traído consigo la aparición de este tipo penal. DOLZ LAGO [69] lo define como: "El las acciones realizadas deliberadamente con el fin de establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor". El segundo aparado del articulo 183 hace alusión a las conductas de *sexting* del siguiente modo: "El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor". La diferencia principal, por tanto, entre este delito y el de *child grooming* es el objeto con el que el sujeto activo establece las comunicaciones con el sujeto pasivo. Como vimos en el *child grooming* el objetivo final del delincuente es abusar sexualmente de un menor mientras que en el *sexting* lo que se pretende es obtener y enviar material pornográfico que contenga la imagen de un menor o menores. DOLZ LAGO [70]nuevamente define el delito de forma sencilla: "intercambio de contenidos pornográficos de menores con un menor de dieciséis años" y afirma que "consistente en el embaucamiento de un menor de dieciséis años a través de las TIC para facilitarle o intercambiar material pornográfico en las que se represente o aparezca un menor."

Para finalizar el último punto es el relativo a los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación. Dicho aparatado se encarga de recoger cualquier otro delito de comisión tecnológica no englobado ya en alguna de las anteriores categorías. Este punto en concreto ha levantado críticas entre la doctrina por considerarlo demasiado abierto. Es cierto que en dicho precepto podrían enmarcarse una pluralidad de acciones, lo cual vendría a

[69] DOLZ LAGO M.J., "Child grooming y sexting: anglicismos, sexo y menores en el Código Penal tras la reforma del 2015", Nº 8758, *Diario La Ley*, 2016, Pág. 5. El autor además explica que el delito no es de comisión instantánea si no que se perpetuación se prolonga en el ejemplo de la tal modo que podemos distinguir una serie de fases dentro del modus operandi. Una primera fase relativa a entablar amistad con el menor y conseguir así cierto grado de confianza. Una segunda fase en la que se recaban datos personales del sujeto pasivo. En la tercera fase el delincuente, manipulando psicológicamente al menor, consigue que el mismo envíe material pornográfico, como por ejemplo fotos de sí mismo desnudo. La última fase, y con las imágenes o videos ya en su poder, el acosador procede a chantajear al menor. Amenaza con sacar a la luz dicho material a no ser que la victima acceda a enviarle más o/y concierte un encuentro físico.

[70] DOLZ LAGO M.J., "Child grooming":…,cit.,p. 4-9

desembocar en inseguridad jurídica para el ciudadano que podría ver limitados sus derechos fundamentales sin que las injerencias sobre los mismos estén claramente delimitadas en la ley. Una de las implicaciones de la amplitud del precepto que más preocupa a algunos autores es el hecho de que el mismo pueda usarse ante la comisión de "delitos menores". En este sentido RUBIO ALAMILLO[71], cuestiona hasta qué punto se ven protegidas las garantías del ciudadano al expresar que: "no se define qué tipología de delitos se enmarca en esta última definición, generando una importante inseguridad jurídica que permitirá intervenir las comunicaciones e instalar programas informáticos intrusivos en los ordenadores de personas que, por ejemplo, escriban determinado tipo de comentarios considerados como peligrosos en foros o en redes sociales." Por el contrario determinadas voces aplauden la flexibilidad de la ley al no configurarse de un modo cerrado, entre ellos RICHARD GONZÁLEZ [72] asevera que "La inexistencia de una penalidad mínima o determinada es correcta, ya que de ese modo se posibilita que, por ejemplo, se pueda acordar la intervención de un teléfono o el registro remoto de un aparato informático para investigar delitos como los de amenazas, coacciones o estafas (cuando se realicen a través de dispositivos electrónicos) que no están castigados con penas elevadas pero que causan daños importantes al conjunto de la sociedad y que, por supuesto, deben ser investigados y juzgados los responsables." Añade el autor, sin embargo, que en el caso de la concreta diligencia de seguimiento y localización sí deberían delimitarse más los presupuestos por ser esta medida, a su juicio, extremadamente invasiva de la privacidad.

A mi juicio esta regulación resulta demasiado amplia y la mayor de las deficiencias de esta ley así como la más peligrosa. Aunque sí que es cierto que, en ocasiones, (especialmente en el campo de las nuevas tecnologías), una regulación abierta de los preceptos legales evita la obsolescencia temprana de las normas, los presupuestos de uso de un tipo de diligencias de investigación tan invasivas no debe ser objeto de indeterminaciones. Como veremos a continuación, en el apartado "Derechos Fundamentales afectados", este tipo de medidas entra en constante colisión con alguna de las garantías más importantes en un estado de derecho. Su uso colisiona inevitablemente con varios Derechos Fundamentales de los ciudadanos que si bien no son absolutos requieren de una necesaria ponderación con otros derechos e intereses del estado antes de ser limitados. Es evidente que para causar injerencias en este tipo derechos y libertades debe existir un fuerte interés que lo justifique. Al configurar la Ley de tal manera que se permita violar Derechos Fundamentales de los ciudadanos siempre que estemos ante "Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación" podría no existir una

[71] RUBIO ALAMILLO, J., "La informática en la reforma de la Ley de Enjuiciamiento Crimina", No 8662, *Diario La Ley*, 2015, pág. 9

[72] RICHARD GONZÁLEZ, M., "Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización", Nº 8808, *Diario La Ley*, 2016, Pág. 15

motivación bastante para considerar legal tal quebrantamiento. No podemos olvidar además que una indeterminación jurídica tan grande ataca al principio de legalidad proclamado en el artículo 9.3 del texto constitucional.[73]

3.4. Derechos fundamentales afectados

Resulta evidente que durante la investigación de los delitos informáticos va a producirse, inevitablemente, una intromisión en la esfera privada de las personas, especialmente si para la misma se utilizan los ya referidos *spywares*. Esta injerencia va a suponer la afectación de determinados Derechos Fundamentales, estos son los derechos comprendidos en la sección primera del capítulo segundo del título primero de la Constitución Española y que gozan de la máxima protección [74] en nuestro ordenamiento jurídico. La propia LO 13/2015 reconoce esta circunstancia y nos delimita que tipos de derechos van a ser los más afectados al rubricar a su TÍTULO VIII "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución" A pesar de su mayúscula importancia intrínseca los Derechos fundamentales no son absolutos [75] debido a que por su propia naturaleza entran en conflicto con otros derechos, en ocasiones también Fundamentales, siendo necesaria en estos casos una ponderación de intereses con el objetivo de discernir qué derecho rima sobre el otro en un concreto caso. Los Derechos Fundamentales en determinados momentos también pueden encontrar sus limitaciones en el interés del Estado, la seguridad pública o la seguridad nacional. Los citados límites permitirán a los cuerpos de seguridad del estado y a los órganos jurisdiccionales emplear diligencias de investigación que puedan llegar a lesionarlos. En este punto debemos hacer referencia a cuáles son los concretos Derechos Fundamentales que pueden

[73] Artículo 9.3 de la Constitución Española: "La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos."

[74] Los Derechos fundamentales se encuentran amparados por una protección constitucional y reforzada consistente en un compendio entre la existencia de un procedimiento especial, preferente y sumario para su tutela (artículo 53.2 CE) y la posibilidad de acudir al recurso de amparo constitucional.
Respecto a la primera de las facetas que conforman su protección por medio de Sentencia de 28 de mayo (STC 81/1992) El Tribunal Constitucional ha concretado los extremos exigidos en este tipo de procedimientos señalando que "la preferencia implica prioridad absoluta por parte de las normas que regulan la competencia funcional o despacho de los asuntos; por sumariedad, como ha puesto de relieve la doctrina, no cabe acudir a su sentido técnico (pues los procesos de protección jurisdiccional no son sumarios, sino especiales), sino a su significación vulgar como equivalente a rapidez". Por su parte el recurso de amparo constitucional (artículo 161.1 b) CE), supone una protección subsidiaria que entrara en juego si los tribunales ordinarios (máximos protectores de los derechos Fundamentales) no logran la efectiva defensa del concreto derecho fundamental.

[75] La Sentencia del Tribunal Constitucional de 8 de abril de 1981 dispone que existen tres tipos de límites a los derechos fundamentales: "La Constitución establece por si misma los límites de los derechos fundamentales en algunas ocasiones. En otras ocasiones, el límite del derecho deriva de la Constitución sólo de una manera mediata o indirecta, en cuanto que ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionalmente protegidos."

verse afectados. VELASCO NUÑEZ [76]señala como los Derechos Fundamentales más afectados por la investigación de los delitos vinculados con las nuevas tecnologías el derecho a la protección de los Datos Personales, el derecho a la intimidad personal y familiar y a la propia imagen el derecho al secreto de sus comunicaciones y el derecho a la inviolabilidad domiciliaria.

Al hacer referencia al derecho a la *protección de datos* nos estamos refiriendo al conjunto de facultades de las que dispone un individuo derivadas de la limitación al uso de la informática recogida el artículo 18.4 de la Constitución[77]. La jurisprudencia del Tribunal Constitucional[78] define este derecho como "el poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quien posee esos datos personales y para qué pudiendo oponerse a esa posesión o uso".

Respecto a la *intimidad personal y familiar* y a la propia imagen, estos derechos se encuentran también el artículo 18 de la Constitución, en concreto en su primer apartado.[79] El derecho a la intimidad se proclama como aquella garantía que nos salvaguarda de las eventuales intromisiones ajenas, producidas por parte de terceros individuos, o por parte de los poderes públicos, en nuestra esfera privada personal y familiar. El Tribunal Constitucional en su Sentencia 170/2013, de 7 de octubre de 2013 [80] define el derecho a la intimidad personal como "una derivación de la dignidad de la persona" y señala que "implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana". Por su parte el derecho a la intimidad guarda una estrecha relación con la propia imagen (como evidencia el

[76] VELASCO NÚÑEZ, E., "Diligencias de investigación penal" en "Delitos cometidos a través de internet", edición nº 1, *Editorial LA LEY*, pág 34.

[77] Artículo 18.4 CE: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

[78] Sentencia 292/2000 de 30 de noviembre del 2000, sobre el recurso de inconstitucionalidad 1463-2000 en la que además de la indicada definición el Tribunal añade que este derecho "se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular"

[79] artículo 18.1 CE que proclama o siguiente: ". Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen."

[80] En esta misma Sentencia añade que "A fin de preservar ese espacio reservado, este derecho "confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido". Así pues, "lo que garantiza el art. 18.1 CE es el secreto sobre nuestra propia esfera de vida personal, excluyendo que sean los terceros, particulares o poderes públicos, los que delimiten los contornos de nuestra vida privada" (STC 159/2009, de 29 de junio, FJ 3; o SSTC 185/2002, de 14 de octubre, FJ 3; y 93/2013, de 23 de abril, FJ 8)."

hecho de que ambos vayan de la mano en el mismo precepto constitucional), impidiendo la captación sin consentimiento de la imagen personal así o de cualquier posterior uso que se haga de esta. El Tribunal Constitucional también ha tenido la oportunidad de pronunciarse acerca de la relación existente entre el registro de un equipo informático y el derecho a la intimidad en su Sentencia 173/2011, de 7 de noviembre de 2011[81] en los siguientes términos: "Si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) –por lo que sus funciones podrían equipararse a los de una agenda electrónica–, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano"

El derecho al *secreto de las comunicaciones* se encuentra consagrado en el párrafo tercero del artículo 18[82] del texto constitucional. El Tribunal Constitucional ha dedicado numerosas resoluciones [83] a concretar los extremos de este Derecho Fundamental, sin embargo cabe poner de relevancia, por su actualidad y su relación con las nuevas tecnologías la Sentencia 115/2013, de 9 de mayo de 2013. En ella se apunta que el secreto de las comunicaciones "consagra tanto la interdicción de la interceptación como el conocimiento antijurídico de las comunicaciones ajenas, por lo que dicho derecho puede resultar vulnerado no sólo por la interceptación en sentido estricto –aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación, de otra forma, del proceso de comunicación– sino también por el conocimiento antijurídico de lo comunicado". Es decir, se puede vulnerar este derecho de dos maneras. O bien interceptando de modo físico los soportes mediante los cuales se realizan las comunicaciones o bien captando el contenido de los mensajes que pretenden transmitirse aunque no se produzca la

[81] En la Sentencia 115/2013 El Tribunal resuelve sobre recurso de amparo planeado ante una condena por el delito de corrupción de menores en la modalidad de distribución de pornografía infantil. Ahondando en los argumentos que el Tribunal esgrime sobre la estrecha relación del derecho a la intimidad y el registro de equipos informáticos este añade: "Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona"

[82] Articulo 18.3**.** Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

[83] SSTC 281/2006, de 9 de octubre, FJ 4; 230/2007, de 5 de noviembre, FJ 2; 142/2012, de 2 de julio, FJ 3, y 241/2012, de 17 de diciembre, FJ 4

apropiación del dispositivo material usado para ello. y añade el Tribunal que este derecho "protege no sólo el contenido de la comunicación, sino también otros aspectos de la misma, como la identidad subjetiva de los interlocutores" también podemos encontrar este derecho reconocido en la Declaración Universal de los Derechos humanos en concreto en el artículo 12[84] de la misma. La jurisprudencia del Tribunal Europeo de los Derechos Humanos (TEDH)[85] ya había declarado años antes que el Tribunal Constitucional (en 1984) que la amplitud del derecho al secreto de las comunicaciones va más allá del contenido de la información trasmitida. Abarca también lo referente a la identidad de los interlocutores, el momento en que se produjo la llamada y durante cuánto tiempo se mantuvo la conversación[86]. En el *caso Malone* se consideró que cuando sobre una llamada o serie de llamadas se aplica un procedimiento conocido como "medición" y que registra el lugar de origen, el destinatario y la duración de la comunicación se está quebrantando el secreto a las comunicaciones que además estaría estrechamente relacionado con el derecho a la vida privada.

Por último también puede verse vulnerado el derecho a la *inviolabilidad domiciliaria*. Este derecho se encuentra enunciado en el artículo 18.2 CE.[87] Se ha declarado por parte de la jurisprudencia constitucional[88] que este derecho cumple la función de garantizar la efectiva realización del derecho a la intimidad personal y familiar y esta función se lleva a cabo otorgando al individuo la facultad de impedir el acceso (o permanencia) a su domicilio a terceros ya sean particulares o los poderes públicos. Este derecho reviste una especial importancia constitucional y por eso en su propia redacción se incluye la imposibilidad de acceder al mismo sin contar con una resolución judicial motivada que lo autorice (al margen de los casos de delito flagrante en los que razones de urgente necesidades permiten la intervención policial inmediata[89]). En ocasiones los virus espía empleados permiten controlar el equipo

[84] Artículo 12 de la Declaración Universal de los Derechos Humanos (1948): "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."

[85] de 2 de agosto de 1984, caso de malone contra el reino unido. (corte europea de derechos humanos de 2 de agosto de 1984) (aplicación no. 8691/79)

[86] En este aspecto la Sentencia declara que: "La medición global de las comunicaciones telefónicas (origen, destino, duración), cuando se efectúan para un fin distinto de su objetivo único de contabilidad, aunque en ausencia de cualquier intervención, como tal, constituye una injerencia en la vida privada."

[87] Artículo 18.2 CE: El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

[88] La STC 22/2003 manifiesta que su jurisprudencia "establece entre la inviolabilidad domiciliaria y el derecho a la intimidad. Desde la STC 22/1984, de 17 de febrero, FJ 2, hemos afirmado que la protección constitucional del domicilio es "una protección de carácter instrumental, que defiende los ámbitos en que se desarrolla la vida privada de la persona"."

[89] Reiterada jurisprudencia del Tribunal Constitucional ha señalado que existen excepciones a la necesidad de autorización judicial en casos de urgencia. Así por ejemplo la Sentencia STC 70/2002, de 3 de abril, en su fundamento jurídico décimo, dispone que: "la regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que sólo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad.

informático para conseguir activarla *webcam* conectada al mismo o el micrófono y captar imágenes y sonidos del interior del domicilio. Recientemente nuestro Tribunal Supremo ha tenido la oportunidad de pronunciarse sobre la magnitud y alcance de este derecho mediante Sentencia 329/2016 de 20 mayo de 2016. En esta el Tribunal considera que el uso de unos prismáticos para vigilar lo que ocurría en el interior de la vivienda de un investigado reviste una intromisión ilegitima en el derecho a la intimidad y la inviolabilidad domiciliaria. De este modo la sentencia declara, en su fundamento de derecho segundo, lo siguiente: "La tutela constitucional del derecho proclamado en el apartado 2 del art. 18 de la CE protege, tanto frente la irrupción inconsentida del intruso en el escenario doméstico, como respecto de la observación clandestina de lo que acontece en su interior, si para ello es preciso valerse de un artilugio técnico de grabación o aproximación de las imágenes. El Estado no puede adentrarse sin autorización judicial en el espacio de exclusión que cada ciudadano dibuja frente a terceros. Lo proscribe el art. 18.2 de la CE. Y se vulnera esa prohibición cuando sin autorización judicial y para sortear los obstáculos propios de la tarea de fiscalización, se recurre a un utensilio óptico que permite ampliar las imágenes y salvar la distancia entre el observante y lo observado." Es evidente como este mismo argumento jurídico podría emplearse para la diligencia de investigación consiste en el acceso remoto a equipos informáticos. En primer lugar se hace alusión al término "observación clandestina". Como ya hemos visto al usar un software espía lo que estamos consiguiendo es precisamente eso, adentrarnos el dispositivo electrónico para acceder a toda la información que este contiene sin que el investigado sepa que está siendo objeto de averiguaciones. Añade el tribunal que la injerencia se comete cuando esta observación clandestina se realice valiéndose de un "artilugio técnico". Precisamente en las diligencias de investigación informáticas es imprescindible el uso de soportes técnicos (el ejemplo más claro son los ordenadores) mediante los cuales configurar y enviar los software espías, recibir y almacenar en ellos la información obtenida por los virus y poder visualizar los datos.) La sentencia rebate también el argumento que asevera que la "no colocación de obstáculos" impide considerar estos actos como una vulneración del artículo 18.2 CE d este modo: "no puede ser neutralizada con el argumento de que el propio morador no ha colocado obstáculos que impidan la visión exterior. El domicilio como recinto constitucionalmente protegido no deja de ser

---

De no existir ésta, los efectos intervenidos que puedan pertenecer al ámbito de lo íntimo han de ponerse a disposición judicial, para que sea el juez quien los examine. Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad".

En el mismo sentido se pronuncia la Sentencia STC 206/2007, de 24 de septiembre , en su fundamento jurídico octavo, al declarar que: "la regla general es que sólo mediante una resolución judicial motivada se pueden adoptar tales medidas y que, de adoptarse sin consentimiento del afectado y sin autorización judicial, han de acreditarse razones de urgencia y necesidad que hagan imprescindible la intervención inmediata y respetarse estrictamente los principios de proporcionalidad y razonabilidad".

domicilio cuando las cortinas no se hallan debidamente cerradas. La expectativa de intimidad, en fin, no desaparece por el hecho de que el titular o usuario de la vivienda no refuerce los elementos de exclusión asociados a cualquier inmueble. Interpretar que unas persianas no bajadas o unas cortinas no corridas por el morador transmiten una autorización implícita para la observación del interior del inmueble, encierra el riesgo de debilitar de forma irreparable el contenido material del derecho a la inviolabilidad domiciliaria" en mi opinión tal argumento es perfectamente exportable a la no colocación de obstáculos en el plano del acceso remoto a equipos informáticos. En este sentido al hablar de obstáculos estaríamos refiriéndonos al uso de antivirus o cortafuegos que impidiesen la instalación de *softwares* espías.

Volviendo sobre las limitaciones al ejercicio de estos derechos cuando las circunstancias lo requieran, las mismas solo operaran cuando se cumplan los requisitos exigidos para ello. Estos presupuestos necesarios para tales restricciones podemos encontrarlos en la tradición jurisprudencial y doctrinal. Como apunta SÁNCHEZ BRAVO[90], los mismos vienen siendo recogidos ya desde lo el Convenio de 1981 del Consejo de Europa[91]. El autor explica como de este texto legal podemos extraer tres requisitos esenciales. El primero la existencia de un fundamento legal que ampare las limitaciones, el segundo la necesaria proporcionalidad en la limitación y que la misma sea imprescindible[92] para alcanzar el respectivo fin legitimo y el tercero impide que se produzca ninguna limitación que por su magnitud suponga un perjuicio al contenido esencial del derecho. Aunque esta la base que debe tenerse en cuenta para todos los derechos fundamentales a partir de ella cada derecho tendrá sus propios requisitos en función sus características propias.

Todo lo expuesto nos lleva a concluir haciendo referencia a la nulidad probatoria de la que adolecerán las pruebas obtenidas mediante diligencias que no respeten los derechos fundamentales. Así viene dispuesto en el artículo 11.1 de la LOPJ[93]. Una prueba nula es aquella que no puede ser tenida en cuenta por el juez a la hora de fundar su decisión, de tan modo que de no existir más pruebas por ella misma no podría enervar la presunción de inocencia. Mediante esta disposición legal se está. Al movernos en el campo de la obtención de pruebas en

[90]SANCHEZ BRAVO, A.A., "El convenio del Consejo de Europa sobre cibercrimen: control vs. libertades públicas", No 5528, *Diario La Ley*, 2002, pág. 18.

[91] Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Artículo 9. "Excepción y restricciones"

[92] Sentencias Lingens, de 8 de julio de 1986; Leander, de 26 de marzo de1987 y Gillow, de 24 de noviembre de 1986 del Tribunal Europeo de Derechos Humanos, que estaremos ante la necesidad de una limitación cuando se produzca exigencia social vital y solo en el caso de que dicha limitación se ajuste en su alcance a la situación de la que deriva su aplicación.

[93] Artículo 11.1 LOPJ **"**En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales."

delitos informáticos VELASCO NÚÑEZ[94] expresa que para que la prueba no adolezca de nulidad debe contarse para su realización con la oportuna autorización judicial, en caso de que esta sea perceptiva, y que solo podrán llevarse a cabo este tipo de diligencias por parte de agentes policiales (suponiendo esto que cualquier obtención de prueba con afección a los derechos fundamentales realizada por un particular será nula). A mi juicio es fundamental contar con una serie de normas, recogidas en la ley, que nos indiquen en qué casos será posible limitar los Derechos Fundamentales y en casos no, así como ciertas pautas que se refieran al modo en que deberá operarse siempre que estas limitaciones sean pertinentes. Si ya ante cualquier tipo de derecho estás cautelas serían necesarias su importancia se vuelve capital si hablamos de Derechos Fundamentales. Será necesario, por lo tanto, y en mi opinión, antes de proceder a vulnerar los Derechos Fundamentales de los ciudadanos constatar que existen razones fundadas para realizar dicha injerencia. Dichos motivos no solo deben basarse en la existencia de una causa si no que el fundamento que motive la intervención de los cuerpos de seguridad a de pasar por una necesaria ponderación extraída de un examen judicial. Deberán llevarse a cabo siempre actuaciones proporcionadas y para ello deberán examinarse detenidamente cada caso concreto, de otro modo podrían cometerse violaciones irreversibles en los derechos más elementales y primordiales de los ciudadanos.

3.5. Supuestos reales y jurisprudencia

Aunque es evidente la capital importancia de estas nuevas formas de investigación basadas en el desarrollo y dominio de las nuevas tecnologías y su utilidad resulta incuestionable, la experiencia práctica nos permite materializar en supuestos reales la teoría que hemos ido exponiendo hasta el momento. Al mismo tiempo que la tecnología evoluciona los delincuentes van adaptando su modus operandi a la misma y empleándola para la comisión de delitos. Yendo un paso más allá existen ciertos delitos que no tendrían cabida sin el empleo de los avances tecnológicos y en concreto de internet. Un ejemplo de este tipo de delitos es el de delito de posesión de material pornográfico (189.5 CP),[95] tipo que suele verse agravado por la conducta de facilitación de la difusión (189.1.b CP) [96] dado que para la obtención del mismo se emplean

[94] VELASCO NÚÑEZ, E., "Diligencias de investigación":…cit,. p. 44.

[95] Artículo 189.5 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal: "El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años."

[96] Artículo 189.1.b de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal:: "El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas

programas P2P[97] en los que cada receptor de material es a su vez emisor. En ocasiones se utilizan métodos de investigación y diligencias ya existentes antes de entrada en vigor de la LO 13/2015 como el registro domiciliario y posterior registro del ordenador. Así por ejemplo la ST 167/2016 [98]de la sala de lo penal del Tribunal Supremo confirma una Sentencia condenatoria de la Sección Primera de la Audiencia Provincial de Zamora, de fecha 06/03/2015 estos delitos.

Sin embargo y aunque en este supuesto no se emplease el uso de virus espía se recogen interesantes conclusiones de la sentencia relativas a los derechos de los investigados asimilables a supuestos en los que se empleasen el acceso remoto. En esta sentencia se explica lo que se tiene en cuenta para considerar que existan o no indicios suficientes para iniciar unas diligencias de investigación: "los oficios expuestos evidencian además la existencia de indicios suficientes para acordar la medida, así como la necesariedad de la misma, puesto que se acreditaron sospechas racionales y fundadas de que en los ordenadores del acusado se había descargado pornografía infantil y por lo tanto era necesario acceder a los mismos y verificar el resultado de la investigación realizada, como efectivamente sucedió. En resumen, la investigación se realizó conforme a la ley, los indicios son sólidos, no se trata de meras sospechas sin fundamento, si bien no puede pretenderse que el auto incorpore hechos probados, pues se trata de una medida que se adopta al inicio de la investigación cuando, dadas las características del delito investigado, no es posible acudir a otras medidas menos gravosas para lograr el buen fin de la investigación". Incidiendo en este tema y en el tipo de presupuestos necesarios para la actuación policial contamos con una Sentencia más actual, ST 40/2016 de 6 abril de la Audiencia

---

personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

[97] En los Fundamentos jurídicos de la Sentencia se explica en qué consiste el funcionamiento de los sistemas P2P: "programas P2P (peer to peer), de los que existen diversas variantes en internet para las distintas redes de intercambio, todas ellas con funcionamiento semejante no existiendo un servidor central en el que se almacenan los contenidos y al que se pueda acceder para evitar su difusión, tratándose de una aplicación que no tiene clientes ni servidores fijos, y si uno de los usuarios inicia la descarga de un archivo, instantáneamente se convierte en servidor de la parte del archivo que ha descargado, posibilitando a un tercero iniciar la descarga simultánea desde su propia carpeta compartida del archivo incompleto recibido"

[98] La propia Sentencia explica en su Fundamento de Derecho primero la forma en la que operó la policía en esta ocasión: "La policía española desarrolló la denominada "operación Ruleta" en el curso de la cual fue identificado el acusado, como uno de los usuarios de la red P2P que realizó conexiones a intercambios de ficheros de contenido pornográfico, al menos en el periodo comprendido entre el 19 y el 23 de marzo de 2008, empleando para ello la red de datos de la operadora JAZZ TELECOM, que le asignó direcciones IP de identificación durante cada sesión asociadas a su número de abonado telefónico. Las conexiones fueron observadas por los investigadores policiales, dado que las redes de intercambio permiten acceder al contenido de los ordenadores desde los que se realizan las conexiones, rutas de acceso definidas libre y voluntariamente por cada usuario para permitir el intercambio de material. Solicitada la correspondiente autorización de entrada y registro del domicilio del acusado, fue autorizada por el juzgado de instrucción número 29 de Madrid mediante auto de fecha 3 septiembre 2009. La entrada y registro se practicó el 23 septiembre del mismo año, en presencia del secretario judicial, dando lugar a la intervención de un ordenador portátil Thimkpad, un ordenador IBM 2373-JXG, de un disco duro Toshiba, de un disco duro Seagate Barracuda, y de un disco duro Fujitsu, todos ellos con contenido pornográfico"

Provincial de Guadalajara (Sección 1ª). En su fundamento jurídico quinto índice en la aplicación de la LO 13/2015 expresando lo siguiente: "lo deseable es que la expresión de los indicios objetivos que justifican la intervención telefónica sea exteriorizada directamente en la resolución judicial, Sin embargo, esa premisa no impide que dicha intervención, según una consolidada doctrina de este Tribunal, cumpla el canon de motivación suficiente si, una vez integrada con la solicitud policial a la que venga a remitirse, contiene los elementos necesarios para poder llevar a cabo con posterioridad la ponderación de la proporcionalidad de la medida (por todas, STC 25/2011, de 14 de marzo FJ 2, y las allí citadas). […] La reforma operada en la LECRIM por la LO 13/2015 de 5 de octubre ha incidido en este extremo al exigir como principio general el de la especialidad que se menciona en el nuevo capítulo IV relativo a las disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, captación y grabación de comunicaciones orales mediante dispositivos electrónicos, utilización de dispositivo técnicos de seguimientos, localización y captación de la imagen, registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos, aludiendo a los principios básicos que han de inspirar estas medidas y que había ido estableciendo la jurisprudencia, especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida apuntando el de especialidad que se ha de referir a la investigación de un delito concreto, no cabe adoptar la medida para prevenir o descubrir delitos o despejar sospechas"

También se aprecian los criterios contenidos en la LO 13/2015 en la Sentencia relativa a un caso de intervención telefónica de las comunicaciones para indagar sobre la introducción de droga en un centro penitenciario. En concreto se basa en el artículo 588 bis a) para referirse a los principios rectores de este tipo de diligencias de investigación. Tras un análisis de todos ellos aplica al caso enjuiciado los principios de excepcionalidad y necesidad recogidos en la ley en los siguientes términos: "En el caso actual nos encontramos precisamente ante un supuesto en el que concurren los principios de excepcionalidad y necesidad, porque la prolongación de la investigación policial externa sin resultados efectivos ha puesto de relieve que no están a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado que el recurso a la intervención de sus comunicaciones". La Sentencia del Tribunal Constitucional 173/2011 de 7 noviembre, por su parte, alude al presupuesto de la necesidad de autorización judicial para el acceso remoto a equipos informáticos en los siguientes términos: "cualquier injerencia en el contenido de un ordenador personal –ya sea por vía de acceso remoto a través de medios técnicos, ya, como en el presente caso, por vía manual– deberá venir legitimada en principio por el consentimiento de su titular, o bien por la concurrencia de los presupuestos habilitantes antes citados." A esta conclusión llega tras analizar la Sentencia del Tribunal Europeo de los Derechos Humanos de

22 de mayo de 2008 referente al caso *Iliya Stefanov* contra Bulgaria en la cual se discutía si el registro del despacho de un abogado y de sus datos físicos y electrónicos suponía una injerencia en el Derecho Fundamental a la intimidad ("a su vida privada" en términos de la Sentencia) que presupuestos eran necesarios para que la intervención policial se considerase legitima.

Entrando ya en el uso de *softwares* de espionaje cabe destacar el uso de un programa llamado "Galileo RCS" (Remote Control System*)* se trata de un producto diseñado por la empresa *Hacking Team* y que fue vendido a los servicios de investigación de más de 35 países.la empresa define este sistema como: "El paquete de hackeo para interceptación gubernamental"[99]. La propia empresa se publicita en su página web del siguiente modo: "Creemos que la lucha contra la delincuencia debe ser fácil: proporcionamos la tecnología ofensiva eficaz, fácil de usar para las comunidades policiales y de inteligencia en todo el mundo."[100] Pero con anterioridad a este software que no deja de ser actual y novedoso ya existían supuestos de este tipo de investigaciones policiales, Uno de los casos más conocidos de investigación policial mediante sistemas de acceso remoto es una operación llevada a cabo por el gobierno estadounidense. Se trata del llamado caso *Scarfo* desarrollado por el FBI en el año 1999 y el cual recibe su nombre en honor al sujeto investigado en él, el conocido mafioso Nicodemo Salvatore Scarfo Jr. Como ya vimos en el punto "Tipos de virus usados y función de cada uno de ellos" el FBI venía utilizando el programa carnívoro para la obtención de información remota sin embargo en este caso dicho programa no tenía utilidad alguna ya que Scarfo utilizaba códigos de encriptación para la emisión y recepción de sus mensajes. Ante esta situación el FBI empleó una nueva estrategia y un nuevo software de espionaje en este caso el *Key Logger System* (KLS) o lector de teclados que como ya explicamos anteriormente consiste en un programa capaz de registrar las pulsaciones de los teclados y así registrar todo lo que se escribe en un determinado equipo. Lo que se pretendía mediante su uso era obtener las contraseñas para desencriptar la información que Scarfo se encargaba de mantener oculta pero en este caso no para registrar los datos que entraban y salían del equipo ni la información almacenada en el disco duro de este[101]. Así el FBI solicito una orden judicial para poder acceder a las oficinas de Scarfo e instalar en su ordenador el programa. Scarfo reaccionó denunció al FBI por un delito de Intervención ilegal de sus comunicaciones sin embargo no prosperó puesto que la información se calificó como secreta por motivos de seguridad nacional y sus abogados no pudieron acceder a la información necesaria para que el caso prosperase.

---

[99] Literalmente en su página web podemos encontrar: "Remote Control System: the hacking suite for governmental interception" http://www.hackingteam.it/index.html. fecha de consulta 18 de agosto de 2016

[100] "We believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities." http://www.hackingteam.it/index.html. fecha de consulta 18 de agosto de 2016

[101] ORTIZ PRADILLO, J.C., "El proceso penal":…cit,.,p. 5.

4. ACTUACIÓN POLICIAL

A la hora de poner en práctica las diligencias que hemos estado desarrollando a lo largo de los puntos anteriores de este trabajo la responsabilidad será de la policía judicial y de los cuerpos de seguridad que ya hemos analizado en el punto 1 (el CNP y la lucha contra el cibercrimen: especial atención a la bit y a la formación especializada). La atribución de esta responsabilidad viene regulada en el artículo 282[102] de la Ley de Enjuiciamiento Criminal el cual atribuye a la policía judicial el deber de investigar delitos y practicar diligencias, entre otros. También en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado se recogen, en el artículo 11.1[103], previsiones semejantes al asignarle la función de "investigar delitos". Quedan por explicar las concretas pautas que seguirán los agentes para efectuar este tipo de medias de investigación. Qué presupuestos deben existir para emprender su actuación, a qué limites van a estar sujetos y haremos una referencia a las cuestiones más problemáticas: la cadena de custodia y el aseguramiento de pruebas.

4.1. Presupuestos y motivación de uso

La LO 13/2015 con el objeto de otorgar seguridad jurídica al empleo de las diligencias de invest0igación que en ella se recogen, especifica los presupuestos que serán necesarios para que las mismas sean legitimas. Para esta tarea hace una división. Por un lado recoge una serie de presupuestos generales, que se emplearan para todas las diligencias recogidas en la ley. Por otro lado especifica los presupuestos que serán necesarios de forma concreta para el uso de virus espía o cualquier otra medida consistente en el registro remoto de equipos informáticos. Comenzaremos haciendo referencia a los presupuestos comunes empezando por el artículo 588 bis a punto uno que recoge los principios a los que deberá sujetarse. Dichos principios no son otros que: especialidad[104], idoneidad[105], excepcionalidad, necesidad [106] y proporcionalidad[107].

[102] Artículo 282 de la Ley de Enjuiciamiento Criminal: "La Policía Judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial. Cuando las víctimas entren en contacto con la Policía Judicial, cumplirá con los deberes de información que prevé la legislación vigente. Asimismo, llevarán a cabo una valoración de las circunstancias particulares de las víctimas para determinar provisionalmente qué medidas de protección deben ser adoptadas para garantizarles una protección adecuada, sin perjuicio de la decisión final que corresponderá adoptar al Juez o Tribunal."

[103] Artículo 11.1 g) de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado: "Investigar los delitos para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del Juez o Tribunal competente, y elaborar los informes técnicos y periciales procedentes."

[104] Este principio viene explicado en el artículo 588 bis a.2 de la LO 13/2015 y supone que la medida solo podrá autorizarse para la persecución de un delito en concreto.

[105] El artículo 588 bis a.3 de la LO 13/2015 dispone que: "el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad." Es decir, que el uso de la medida se ajusta a la necesidad de investigación y que la medida es útil para la consecución del fin que se persigue.

Ahondando aún más en estas exigencias la ley en el punto dos da una explicación de lo que se entiende por cada uno de estos principios y por tanto cuando podemos afirmar que nos encontramos en una situación encuadrable en ellos.

El segundo presupuesto general, contenido en el artículo 588 bis b, es la solicitud de autorización judicial. Al tratarse de medidas que necesariamente han de ser autorizadas por un juez (como veremos más adelante en los presupuestos específicos) es evidente que deberá solicitarse al mismo que dicte resolución al respecto, en el caso de que actúe a instancia de parte (el juez también podrá actuar de oficio [108]en este caso, lógicamente, no será necesaria). La solicitud, que podrá ser enviada por el Ministerio Fiscal o la Policía Judicial deberá contener una descripción de los hechos objeto de la investigación, del investigado y otros afectados por la medida, los motivos por los cuales la medida resulta *necesaria* incluyendo los indicios existentes, los medios de comunicación empelados para ejecutarla, el alcance de la medida, la identificación de la unidad investigadora a cargo de la misma, el modo en que se ejecutara, su duración, y, para acabar, el sujeto que la llevara a cabo, si ya se conoce en ese momento.

Entrando ya a analizar los presupuestos específicos el principal es que esté tratando de investigarse un tipo de delito concreto. No ante indicios de comisión de cualquier tipo delictivo pueden llevarse a cabo este tipo de diligencias. Como ya vimos y explicamos en el apartado "tipo penal y ámbito de aplicación" la LO 13/2015, en su artículo 588 septies, punto uno desglosa una lista enumerando los actos criminales para los que estas diligencias son de aplicación. A fin de no resultar redundantes nos remitiremos a lo ya expuesto sobre el tipo delictivo y nos centraremos en el segundo presupuesto que aún no se ha mencionado, también recogido en el artículo 588 (punto dos en este caso) no en vano rubricado "presupuestos". El segundo requisito indispensable, por tanto, para poder proceder a la instalación de un software espía en el equipo informático de un sospechoso es contar con una resolución judicial motivada que autorice la medida. La resolución deberá contener información detallada sobre los

[106] Los principios de excepcionalidad y necesidad vienen recogidos bajo el mismo precepto, el artículo 588 bis a.4 de la LO 13/2015. El primer apartado de este precepto explica el principio de excepcionalidad al decir que solo podrá emplearse esta medida siempre y cuando no exista alguna otra menos gravosa para el investigado. El segundo apartado y haciendo referencia al principio de necesidad del siguiente modo: "cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida" o lo que es lo mismo cuando la investigación presenta grandes dificultades sin el uso de la diligencia.

[107] Según el artículo 588 bis a.4 de la LO 13/2015 una medida será proporcionada cuando tras ponderar y los intereses del estado y de terceros y los derechos del investigado o investigados en el caso no se produzcan vulneraciones o injerencias excesivas en los mismos. Además la ley, concreta que parámetros deberán tener en cuenta para la referida ponderación: "la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho."

[108] Artículo 588 bis b.1 LO 13/2015

siguientes extremos: en primer lugar una enumeración de todos los equipos informáticos sobre los que vaya a recaer la diligencia, en segundo lugar deberá especificarse en qué consiste la medida es decir "El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información"[109] en tercer lugar la identificación de los agentes que realizarán las diligencias, en cuarto lugar en caso de que no solo se quiera conocer la información si no que se quiera hacer copia de la misma se deberá solicitar concretamente, en quinto y último lugar otras medidas adicionales que sean necesarias para conservar los datos obtenidos o en su caso también para eliminarlos del equipo informático de origen. Para terminar con los presupuestos especiales, en caso de que la medida pretenda ampliarse a otros equipos deberá solicitarse, al juez competente, dicha ampliación.

4.2. Límites a la actuación policial

El límite básico al que esta diligencia de investigación debe acogerse no es otro que un límite temporal. El artículo 588 septies c de la LO 13/2015 dispone que "La medida tendrá una duración máxima de un mes". Es posible que en determinados casos, debido a la complejidad de los mismos, la investigación deba prorrogarse. Es por eso que este mismo artículo prevé esa posibilidad y añade que será posible la prorroga por periodos iguales al mes pero con un límite máximo absoluto: tres meses de duración. En cualquier caso no debemos olvidar lo dispuesto en el artículo 588 bis e, que obliga a emplear solo la medida durante el tiempo "imprescindible para el esclarecimiento de los hechos."

Otro de los límites a la actuación policial es el sometimiento al control y seguimiento judicial. Como ya hemos explicado en el apartado "Derechos Fundamentales afectados" en el secreto de las comunicaciones el grado de injerencia de este tipo de medidas es elevado. El Tribunal Constitucional ha sentado doctrina con respecto a las garantías que asisten a los titulares de este derecho. A titulo ejemplificativo la sentencia 9/2011, de 28 de febrero de 2011, que a su vez remite a la Sentencia 165/2005, de 20 de junio, dispone que: "el control judicial de la ejecución de la medida de intervención de las comunicaciones se integra en el contenido esencial del derecho al secreto de las comunicaciones". La LO 13/2015 resuelve que este se llevara a cabo mediante informaciones periódicas al juez encargado de la instrucción. La prioridad de estos informes sobre los avances que se vayan realizando la determinará el juez y además la policía judicial está obligado a informa en todo caso siempre que la medida finalice. Así viene dispuesto en el artículo 588 bis g, enunciado: "control de la medida".

[109] Artículo 588 septies a. 2 b LO13/2015

Otro de los límites a los que la actuación policial debe someterse son los llamados hallazgos causales, tema que por su importancia desarrollaremos más detenidamente a continuación. Como es lógico, al introducir un software espía en el ordenador de un investigado, la cantidad de información a la que se tiene acceso es muy amplia. Por este motivo no es raro que en ocasiones se descubran ciertos indicios de comisión de delitos diferentes a aquellos para los que se emitió autorización judicial. En el supuesto de que esto ocurra la policía judicial no puede continuar por su cuenta la investigación de estos indicios. BONILLA CORREA define el hallazgo causal como: "descubrimiento de un elemento de prueba referido a un delito distinto a aquel por el cual se ha concedido el registro durante la diligencia de registro. Se trata, por tanto, de la obtención de una prueba mientras se está investigando otro delito, distinto de aquel por el que se estaba legitimado para practicar la diligencia". BUENO DE MATA [110] por su parte, los conceptualiza (en una definición, a mi juicio, que recoge de forma más concreta la verdadera problemática de esta figura) como: "la aparición de hechos delictivos nuevos y no incluidos en la resolución judicial habilitante de la medida de intervención electrónica, que surgen a la luz de la investigación que se está llevando a cabo." Se trata por tanto de pruebas, obtenidas sin resolución judicial expresa, surgidas a raíz de investigar una prueba originaria para la que sí existía autorización. De la simple lectura de esta definición podemos darnos cuenta que los hallazgos causales suponen una colisión con uno de los principios rectores enunciados en el artículo 588 bis de la LO13/2015 y que ya hablamos en el punto "presupuestos y motivación de uso" este es el principio de especialidad consistente en que la medida solo podrá ser autorizada para delitos concretos y específicos y no para una generalidad de delito indeterminada. Esto vendría a suponer que sí se descubre un la comisión de un delito no contemplada en la autorización judicial se estaría quebrantando el principio de especialidad y con él los derechos fundamentales del investigado. Es por este motivo que decidir como deberían tratarse los hallazgos causales ha cosechado distintas opiniones entre la doctrina. VELASCO NUÑEZ [111] considera que la fase de instrucción se basa precisamente en investigar y por tanto descubrir la comisión de delitos por lo que resultaría contraproducente ajustarse de forma rígida a los tipos sospechados por la policía y que la labor de esta se limitara a confirmar sus hipótesis criminológicas. Considera el autor que del descubrimiento de estos hallazgos se deriva tanto para el juez como para los cuerpos de seguridad la "obligación" de investigarlos. Apoyándose en jurisprudencia del Tribunal Supremo[112] este autor considera que si la autorización judicial

[110] BUENO DE MATA F., "Comentarios y reflexiones": …,cit.,p. 3
[111] VELASCO NÚÑEZ, E., "Diligencias de investigación":…cit,. p. 7.

[112]STS 1611/1997 de 29 de diciembre de 1997. En esta sentencia se produce un hallazgo causal durante una diligencia de intervención telefónica. El Tribunal resuelve la causa del siguiente modo: "En relación con el hecho de que en una intervención telefónica legítimamente practicada en otra causa se hubiesen obtenido datos que orientaran la investigación hacia el recurrente, esta Sala ya ha señalado que el descubrimiento casual de indicios de otro delito distinto del investigado durante un registro domiciliario o

fue emitida conforme al principio de proporcionalidad y respetando todas las exigencias del ordenamiento jurídico (excluyendo así un posible uso fraudulento de la diligencia) los hallazgos causales tendrán plena validez probatoria. Por su parte BUENO DE MATA señala que lo relevante a la hora de decidir si un hallazgo causal puede ser considerado una prueba obtenida conforme a derecho es el criterio de conexidad, es decir que el "hecho constituya un delito relacionado con el inicialmente investigado"[113]. Para este autor el criterio de conexidad daría lugar a dos situaciones diferenciadas. Aquellas en las que si existiera relación entre delitos requerirían tan solo una ampliación de la orden judicial inicial mientras que las que no se diera tan conexión el juez debería emitir una orden expresa y enfocada a un nuevo delito dando ligar así a una nueva causa. VELASCO NUÑEZ, sin embargo y en la línea de sus argumentos, aboga por un modo de proceder diferente en el caso de hallarse ante un hallazgo causal sin conexidad (o con él lo llama sin "homogeneidad delictiva"): "debe procederse evitando la continuación de la existencia del nuevo delito hasta entonces ignorado, pero la ocupación debe interrumpirse también, ponerse en comunicación de la autoridad judicial ordenante y, en su caso, conseguir de ella un complemento de mandamiento razonado, que puede ordenarse de forma oral (que debe unirse de forma razonada a autos con posterioridad), para proceder también contra el delito casualmente descubierto y con ello conseguir que la aprehensión del «hallazgo casual» tenga la cobertura necesaria de la garantía constitucional que supone la intervención judicial ."[114] El artículo 588 Bis i, de la LO 13/2015 (mediante remisión al artículo 579 bis) adopta una posición concordante con la del autor BUENO DE MATA. Dispone respecto de los hallazgos causales que los mismos solo podrán continuar siendo investigados si el juez dicta resolución que lo autorice. Para su emisión el juez deberá valorar tres parámetros: la diligencia de la actuación (es decir que la medida investigadora se haya desarrollado correctamente), el marco en el que se produjo el hallazgo (la situación que envolvía al nuevo descubrimiento) y la imposibilidad de haber solicitado la medida que lo incluyera en su momento).

---

una intervención telefónica no implica vulneración de los derechos fundamentales garantizados por el art. 18 de la Constitución Española, siempre que se cumpla el requisito de proporcionalidad y que la autorización y práctica del registro o de la intervención se ajustan plenamente a las exigencias y prevenciones legales y constitucionales, como sucede en el caso actual (sentencias de 28 de abril, 7 de julio y 1 de diciembre de 3 1.995, 4 y 31 de octubre de 1996 y 26 de septiembre de 1997, entre otras). No concurriendo, en consecuencia, violación alguna de derechos fundamentales en la obtención casual de indicios utilizados como instrumento de la investigación inicial"

[113] BUENO DE MATA F., "Comentarios y reflexiones": …,cit.,p. 3

[114] VELASCO NÚÑEZ, E., "Diligencias de investigación":…cit,. p. 7.

4.3. Cuestiones problemáticas: cadena de custodia y aseguramiento de pruebas: hacia un posible diseño de un protocolo de actuación en este tipo de delitos.

Antes de entrar a analizar estas cuestiones es importante delimitar con anterioridad el concepto de prueba electrónica y detenernos en sus particularidades, ya que es sobre la base respecto a la cual analizaremos la cadena de custodia y el aseguramiento, siendo, por tanto, su entendimiento clave para el estudio de este capítulo. DAVARA RODRIGUEZ [115] define a la evidencia informática como "indicios o rastros informáticos que llevan a conocer una acción y a asegurar un resultado a través de información contenida en el propio ordenador"

Por su parte, aportando un concepto en mi opinión más rotundo y pormenorizado al cual llega tras un exhaustivo estudio de las definiciones que se han dado entre la doctrina y otros sectores entendidos en la materia (tanto a nivel nacional como internacional) , BUENO DE MATA[116] conceptualiza la prueba electrónica como: "aquel medio electrónico que permite acreditar hechos relevantes para el proceso, ya sean hechos físicos o incluso electrónicos, y que se compone de dos elementos necesarios para su existencia, los cuales determinan la especialidad de la prueba electrónica en relación al resto de medios probatorios: un elemento técnico o , y un elemento lógico o . La prueba electrónica se presenta así a hardware software través de un soporte electrónico, que va a incluir un contenido informativo elaborado a través de un programa informático determinado" el autor añade que, en base a esta definición, podemos encontrarnos con dos tipos distintos de prueba electrónica en función de los hechos que evidencien cada una, así por un lado tendríamos la prueba electrónica que prueba la existencia de hechos físicos y por otro aquella que prueba hechos electrónicos. Continua BUENO DE MATA exponiendo tanto las ventajas como los inconvenientes de este medio probatorio, lo cual ayuda a concretar aún más en las especialidades de esta figura y termina completar la descripción del mismo. Respecto a las ventajas, y a grandes rasgos, el autor señala la claridad, objetividad y certeza que aporta este tipo de evidencias apunta también su adaptabilidad a todos los órdenes jurisdiccionales y su gran utilidad en cada uno de ellos. Además su obtención resulta más sencilla que en otro tipo de pruebas debido a su automatización lo cual acaba derivando en una última ventaja: la economización del proceso tanto a nivel de costes como a nivel temporal. En relación a las desventajas BUENO DE MATA las divide en dos grupos: legales y técnicas. En cuanto a las legales podemos resumir su argumentación señalando la falta de seguridad jurídica que provoca la necesidad de mejoras legales en la materia que a día de hoy aún cuenta con importantes lagunas legales. Con respecto a las técnicas, lo más destacables la

[115] DAVARA RODRÍGUEZ, M.A., "Las videncias electrónicas", Nº 20, *Editorial LA LEY*, 201,1 pág. 24-28,

[116] BUENO DE MATA, F., "Prueba electrónica y proceso 2.0. Especial referencia al proceso civil", *Tirant lo Blanch*, 2014, Pág. 14

necesidad de contar con conocimientos en las TIC, lo que desemboca en la necesidad de requerir asistencia pericial (muchas veces limitada por la escasez de recursos tecnológicos en los juzgados), la facilidad de modificación de las mismas y la desconfianza que esta produce en su autenticidad. En definitiva, es característica propia de las pruebas que pueden obtenerse al investigar este tipo de hechos delictivos su mudable integridad, al ser los datos contenidos en dispositivos electrónicos extremadamente susceptibles de alteración. Es por esto motivo que el aseguramiento de las pruebas y su cadena de custodia reviste peculiaridades y exige mayor rigor que otro tipo de material probatorio.

Respecto del aseguramiento de prueba podemos encontrar esta cuestión regulado en el articulo 588 octies de la LO 13/2015.[117] Por medio de este precepto se faculta a la policía judicial y al Ministerio Fiscal a ordenar a "cualquier persona" la conservación de datos que obren en su poder de tal modo que si no lo hiciesen incurrirían en las mismas responsabilidades previstas que para el quebrantamiento del deber de colaboración del Artículo 588 ter e. Este artículo está configurado para los supuestos en que, por falta de la oportuna autorización judicial, no pueda producirse la cesión de los datos y exista la posibilidad de que estos puedan perderse. Se trata de garantizar que los datos no van a desaparecer y que van a poder ser recabados cuando puedan recogerse respetándose las garantías procesales. La ley no hace más precisiones para concretar en qué consiste el aseguramiento y conservación de las pruebas pero sí delimita la extensión temporal de la medida estableciendo como plazo máximo un periodo de 90 días. Se configura la posibilidad de una prorroga de igual duración siendo el máximo absoluto los 180 días.

Para poder abordar las especialidades existentes en este ámbito es importante definir en primer lugar el concepto "cadena de custodia". Al hacer referencia a este término estamos hablando de la sucesión de actos encaminados a impedir la modificación del material probatorio una vez recogido y hasta su análisis pericial. La importancia que reviste esta cuestión es clave desde el plano de las garantías procesales del investigado de tal modo que si no se respeta esta cadena la evidencia perderá toda su validez probatoria. La Ley de Enjuiciamiento Criminal recoge esta cuestión en su artículo 338 a proclamar la necesidad de garantía de la integridad del material probatorio de la siguiente manera: "Sin perjuicio de lo establecido en el Capítulo II bis

[117] Artículo 588 octies de la LO 13/2015: "El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes. Los datos se conservarán durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días. El requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, quedando sujeto a la responsabilidad descrita en el apartado·3 del artículo 588 ter e.»

del presente título, los instrumentos, armas y efectos a que se refiere el artículo 334[118] se recogerán de tal forma que se garantice su integridad y el Juez acordará su retención, conservación o envío al organismo adecuado para su depósito".

EIRANOVA ENCINAS [119] explica que, "desde que se recogen los vestigios relacionados con el delito, y hasta que llegan a concretarse como pruebas en el momento del juicio, debe garantizarse que «aquello» sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio de los juzgadores, es lo mismo". El Tribunal Supremo en su Sentencia STS 257/2007 de 26 de marzo de 2007[120] señala que lo determinante para considerar si se ha respetado o no la cadena de custodia es que el material objeto de pericia sea el mismo que el extraído. Señala también, en su sentencia STS 1045/2011, de 14 de octubre que "El problema que plantea la cadena de custodia, hemos dicho en STS 6/2010, de 27-1 , 776/2011 de 20-7 , es garantizar que desde que se recogen los vestigios relacionados con el delito hasta que llegan a concretarse como pruebas en el momento del juicio, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio del tribunal es lo mismo; es decir, es necesario tener la seguridad de que lo que se traslada, analiza o, en este caso, se visiona, es lo mismo en todo momento, desde que se interviene hasta el momento final que se estudia y analiza."

Para garantizar esta identidad es necesario extremar las cautelas desde el mismo momento de la recogida u obtención de la prueba. En caso de que esta pueda aprehenderse de forma física (por ejemplo, incautación de un ordenador o de un disco duro) esta debe colocarse en contenedores adecuados y debe procederse a su correcto etiquetado para una identificación y estudio posterior exento de errores cómo se haría con cualquier otra prueba no electrónica[121]. Este procedimiento ya se lleva a cabo en países de tradición anglosajona como Estados Unidos e Inglaterra. Para que se cumpla esta efectiva identidad sustancial las precauciones que se toman en el plano de la prueba tecnológica, como indica VELASCO NUÑEZ[122], son principalmente dos: (siendo la base común a ambas es el clonado del disco duro) "En las pericias informáticas

[118] Los instrumentos, armas y efectos a los que se refiere el artículo 334 de la Ley de Enjuiciamiento Criminal son: "… las armas, instrumentos o efectos de cualquiera clase que puedan tener relación con el delito y se hallen en el lugar en que éste se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida."

[119] EIRANOVA ENCINAS, E., "Cadena de Custodia y Prueba de Cargo", Nº 6863, *Diario La Ley*, 2008, Pág.4

[120] En el Fundamento de Derecho Primero la Sentencia declara que: "B) Igualmente, y de acuerdo con lo documentado en autos, al margen de la mayor o menor escrupulosidad con la que se cumpliera el protocolo previsto para ello, lo cierto es que no puede albergarse duda alguna acerca de que la droga analizada fue, realmente, la misma que se le ocupó al recurrente, cuando circulaba al volante de su vehículo"

[121] CUADRADO SALINAS, C. "Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa", Nº 107, *Editorial LA LEY*, 2014, Pág. 7

[122] VELASCO NÚÑEZ, E., "Diligencias de investigación":…cit,. p. 44.

que aquí tratamos, técnicamente esto se consigue con el copiado en modo de solo lectura (no modificable), o se verifica contrastando el resumen digital recogido sobre la prueba original (basado en algoritmos hash) con el de la copia sobre la que se va a emitir la pericia". Por lo tanto la primera cautela se basa en lo siguiente: a la hora de realizar los análisis de la prueba estos se llevaran a cabo sobre versiones que impidan las alteraciones en el contenido de la misma. Por otra parte, la segunda cautela se realiza para asegurarnos que entre el material recogido y el analizado existe una absoluta correspondencia. La total identidad se produce cuando la copia se lleva a cabo bit a bit, siendo el bit la unidad mínima de almacenamiento de datos en informática y demás tecnologías digitales. A esta certeza se llega mediante una comparación de los algoritmos hash (también llamados técnica MD5 y SHA1[123]) de la prueba inicial y de su copia objeto de estudio. Los algoritmos hash se extraen mediante el uso de un software matemático que crea un código de identificación alfanumérico que compartirán la prueba original y su clon. De este modo la sola alteración, eliminación de un bit así como la aparición de uno o más bits nuevos arrojarían códigos hash distintos. Será imprescindible que la cifra numérica arrojada por el soporte original y por la copia sea idéntica.

Es importante a su vez que el disco duro original del que se han extraído los datos objeto de la pericia sea precintado durante el proceso. Esta precaución es muy importante de cara a la realización de segundas pericias contradictorias. En el caso de que se produjeran alteraciones en el disco duro original los resultados que arrojaría el segundo volcado de datos para la realización de una nueva pericia no coincidiría con el primero y esto acarrearía que la prueba fuera considerada nula. Para acabar de garantizar la máxima certeza en la prueba pericial el disco duro en el que se "vuelquen" los datos no debe haber sido usado con anterioridad si no que debe desprecintarse en el mismo momento de llevar a cabo la copia y preferiblemente puesto a disposición del perito por el juzgado.[124] Estas dos cautelas, sin embargo, como bien indica VELASCO NUÑEZ[125], no son las únicas. La fe pública que otorga el secretario judicial

[123]Una explicación más exhaustiva sobre el funcionamiento de la técnica MD5 la encontramos en ALVAREZ SERNA, A., MARTIN RIVERA, O.D., VICTORIA MORALES J.D., "Framework para la computación forense en Colombia". Nº2, *USBMed*, 2012, pág. 67.: "El paso siguiente después de la recolección de la información es establecer un mecanismo mediante el cual podamos asegurar la integridad de los datos, para este propósito son utilizados los algoritmos de resumen como el MD5 y SHA1 que arrojan como resultado un valor alfanumérico de longitud fija llamado HASH, estos algoritmos pueden recibir como entrada una cadena de caracteres ó archivos de cualquier tamaño y permiten asegurar que los documentos digitales no han sido alterados durante la investigación". Este tema también ha sido abordado por VIDE. LUEHR, P.H., "Real Evidence, Virtual Crimes. The role of Computer Forensic Expert", N.o 20, *Criminal Justice*, 2005- 2006, p. 17. El investigador señala que este procedimiento es más fiable incluso que los análisis de ADN puesto que la posibilidad de generar al azar dos claves idénticas es de una entre 140 trillones.

[124] SANZ-GADEA GÓMEZ, J.B., "Los informes periciales informáticos en el ámbito de las nuevas tecnologías y prueba ilícita" Nº39, *Revista Jurídica de Canarias*,2015, pág. 69

[125] VELASCO NÚÑEZ, E., "Diligencias de investigación":…cit,. p. 83: Añade el autor expresa la idea de que siempre es conveniente garantizar la integridad de la prueba lo más cuidadosamente posible y por ello

será clave, tanto en el momento de la recogida del disco duro, como cuando se produzca el desprecinto del mismo dentro de las dependencias policiales. En el paso posterior es donde entra en juego el clonado de los datos que es la base común a las dos cautelas ya vistas (realizar la pericia sobre una copia y usar algoritmos hash para asegurar la identidad entre la copia analizada y el original). BONILLA CORREA[126] define el volcado de datos como "una diligencia judicial que se realiza durante la fase de investigación, y que tiene una condición autónoma respecto de la diligencia de registro. Con ella lo que se busca es garantizar la identidad e integridad de lo intervenido". Durante el proceso de clonado o volcado de datos deberá estar presente el letrado de la administración de justicia.

La cadena de custodia y la garantía de presencia de fedatario público en determinados momentos de la misma, ha sido abordada también por el Tribunal Constitucional. Cada mencionar al respecto su sentencia 170/2003[127] en la cual se dispone que: "Del mismo modo que la ausencia de control judicial de las cintas lesiona el derecho al secreto de las comunicaciones (SSTC 121/1998, de 15 de junio, FJ 3; 49/1999, de 5 de abril, FJ 11), aquí la ausencia de control vicia la pertinencia de la prueba. Aquí no estamos ante una garantía meramente legal, sino ante una que afecta a la validez constitucional de la prueba." El Tribunal Supremo también se ha pronunciado al respecto en su Sentencia STS 285/2016: "Ciertamente la realización del volcado a presencia del secretario judicial no acredita el contenido de los soportes digitales pero sí que el material analizado por los agentes versa precisamente sobre el contenido de esos discos duro"

El Tribunal Supremo ha delimitado también en que momentos de la cadena de custodia será imprescindible la presencia del fedatario público y en cuales no mediante su Sentencia 1599/1999 de 15 de noviembre de 1999 "Lo que no se puede pretender es que el fedatario público esté presente durante todo el proceso, extremadamente complejo e incomprensible para un profano, que supone el análisis y desentrañamiento de los datos incorporados a un sistema informático. Ninguna garantía podría añadirse con la presencia del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia." Por lo tanto posterior análisis del contenido, cuando se

indica que: "Si la información se corporeiza -por ejemplo, imprimiéndola- en el momento de su ocupación en la diligencia de entrada y registro, con presencia del secretario judicial (lo cual siempre dentro de lo posible se recomienda, sobre todo en los casos en que se realiza a presencia de imputado claramente identificado), los documentos aprehendidos cuentan con el reforzamiento probatorio de la fe pública.

[126] BONILLA CORREA. J.A., "Los avances tecnológicos y sus incidencias en la ejecución de la diligencia de registro en domicilio", Nº 8522, *Diario La Ley*, 2015, Pág. 11

[127] SENTENCIA 170/2003, de 29 de septiembre de 2003 (BOE núm. 254 de 23 de octubre de 2003) Fundamento Jurídico tercero.

trate de un gran volumen de datos, no requerirá ya de la presencia de este fedatario público, decisión lógica puesto que el mismo se basaría en conocimientos técnicos de los que muy probablemente el secretario judicial carezca, por su posible prolongación en el tiempo y porque lo determinante es que el mismo de fe del copiado idéntico entre la prueba original obtenida.

Sin embargo, cabe añadir que aunque existan esta cautelas y la jurisprudencia ya mencionada y aplicable al respecto, del estudio de la LO 13/2015 se desprende que no existe una previsión legal concreta que determine un procedimiento común para la cadena de custodia. Esto vendrá a significar que las circunstancias concretas de cada caso serán las que dictaminen la forma de operar. En este sentido la ya mencionada Sentencia STS 257/2007 declara que "Deben pues examinarse los momentos de recogida, custodia y examen de las piezas de convicción o cuerpo u objeto del delito a efectos de determinar la concreción jurídica de la cadena de custodia. Lo hallado deber ser descrito y tomado con las debidas garantías, puesto en depósito con las debidas garantías y analizado con las debidas garantías" sin embargo no da pautas de cómo deben llevarse a cabo estos trabajos ni remite a norma alguna que lo haga.

A falta de regulación legal en esta materia se han ofrecido de forma más informal ciertas normas referidas al análisis forense de la prueba electrónica. Así por ejemplo podemos destacar la aportación de AENOR[128] que mediante el comité técnico AEN/CNT 71 redactó en el año 2013 la norma UNE 71506:2013 [129]. Cómo la propia norma indica en el apartado relativo al objeto de la misma su cometido es "establecer una metodología para la preservación, adquisición documentación, análisis y presentación de evidencias electrónicas" en el documento se hace hincapié en la necesidad de establecer protocolos que garanticen la integridad de las pruebas. El necesario clonado de los datos es otro de los puntos a los que más importancia da la norma.

En la misma línea, CUADRADO SALINAS,[130] expresa la importancia de contar con un protocolo de actuación detallado que recoja todas las cuestiones relativas a la cadena de custodia. Menciona esta autora otros países[131] en los que se siguen estas pautas y da las claves

[128] AENOR se define a sí misma en su página web como: "La Asociación Española de Normalización y Certificación es una entidad privada sin fines lucrativos que se creó en 1986. Su actividad contribuye a mejorar la calidad y competitividad de las empresas, sus productos y servicios.
AENOR, a través del desarrollo de normas técnicas y certificaciones, contribuye a mejorar la calidad y competitividad de las empresas, sus productos y servicios, de esta forma ayuda a las organizaciones a generar uno de los valores más apreciados en la economía actual: la confianza." http://www.aenor.es/aenor/aenor/perfil/perfil.asp#.V63dt_mLTIU fecha de consulta 12 de agosto de 2016

[129] Con fecha de edición 2013-07-03, el título en español de esta norma es: "Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas."

[130] CUADRADO SALINAS, C. "Registro informático":…cit.,p.7.

[131] CUADRADO SALINAS, C. "Registro informático":…cit.,p.7.De forma ilustrativa CUADRADO SALINAS apunta: "En Inglaterra, por ejemplo, la policía (ACPO), recoge tales procedimientos en la Guía de Buenas Prácticas para recabar datos probatorios de equipos electrónicos, y en los Estados Unidos el

que deberían seguirse para prevenir errores. Explica, además, que es conveniente apuntar los datos sobre el contexto de recogida de las evidencias, método de custodia empleado, procesos técnicos que se ejecutaron sobre ellos para su estudio, relación cronológica de la cadena de hechos, y por su puesto identificación de los peritos intervinientes. Por medio de una exhaustiva documentación de logra más seguridad jurídica en torno a la cadena de custodia y los estándares de garantía que deben de regir en la misma. Los países en los que ya se llevan a cabo estas prácticas (los ya mencionados Estados Unidos e Inglaterra) reflejan todos estados datos en un "documento esencial" que completa su formalización incluyendo las firmas de los intervinientes en la cadena de custodia.

Por su parte JUAN BAUTISTA SANZ-GADEA GÓMEZ[132] considera que para garantizar la máxima pureza de la prueba pericial el instrumental empleado para la realización de la misma debe estar convenientemente esterilizado de tal modo que *"Los medios técnicos a utilizar por los forenses informáticos deben estar certificados, hayan sido expuestos a variaciones magnéticas, ópticas (laser) o similares, para evitar que las copias de las evidencias obtenidas puedas estar contaminadas"*. Del mismo modo hace hincapié en la necesidad de que el software empleados hayan sido probados con anterioridad y que existan datos de evaluadores científicos con respecto a su tasa de efectividad. Añade este autor que el perito debe reflejar de forma exhaustiva todos los resultados obtenidos en su examen. Esto implica que no solo debe hacer constar lo que encuentra si no también lo que "no encuentra" cuando existan indicios de que determinados ficheros hayan podido ser borrados. Así si se detecta la instalación de programas de "borrado seguro" (softwares que permitir eliminar datos de forma definitiva, absoluta e irreversible) esta circunstancia deberá figurar en su informe.

Como hemos venido adelantando, la importancia de esta cuestión reside en que si no se respeta la cadena de custodia estaríamos quebrantado un importante requisito de validez de prueba. La consecuencia inmediata derivada sería la nulidad de la prueba lo que podría acarrear incluso la libre absolución del investigado por falta de material probatorio licito. Al mismo tiempo estas cajuelas son necesarias para evitar que se produzca un uso torticero y fraudulento de las diligencias de investigación. Así se garantizan los derechos de los investigados, destacado el derecho a una defensa justa. El Tribunal Constitucional así lo ha reflejado en su Sentencia 170/2003, de 29 de septiembre de 2003[133] en cuyo fundamento jurídico tercero recoge: "Del

---

Departamento de Justicia, publicó en noviembre de 2009, el protocolo sobre investigación en el lugar del delito electrónico".

[132] SANZ-GADEA GÓMEZ, J.B., "Los informes periciales":…cit.,p.70.

[133] En esta Sentencia se estudia si las pruebas recogidas en un caso de delito contra la propiedad intelectual habían respetado o no la cadena de custodia y con ella "el cumplimiento de las garantías procesales en la incorporación al procedimiento penal de los soportes informáticos incautados y los informes periciales realizados sobre ellos". Durante la recogida del material probatorio los afectos

mismo modo que la ausencia de control judicial de las cintas lesiona el derecho al secreto de las comunicaciones (SSTC 121/1998, de 15 de junio, FJ 3; 49/1999, de 5 de abril, FJ 11), aquí la ausencia de control vicia la pertinencia de la prueba. Aquí no estamos ante una garantía meramente legal, sino ante una que afecta a la validez constitucional de la prueba. Por tanto, este concreto motivo de amparo debe ser estimado y, en la medida en que se han valorado como actividad probatoria de cargo los informes periciales efectuados sobre un material informático que se incorporó sin que quedara acreditado el cumplimiento de las debidas garantías de custodia policial y control judicial sobre su identidad e integridad, debe declararse que se ha vulnerado el derecho a un proceso con todas las garantías."

Como vemos nuevamente la ley cuenta con una regulación insuficiente en este aspecto. Si bien resulta, en mi opinión, menos problemática en este aspecto que en otros anteriormente señalados (como la falta de concreción en el último de sus los presupuestos y motivación de uso) vuelve a comportar inseguridad jurídica. La creación de la LO 13/2015 habría sido una oportunidad ideal para dar pautas acerca de la cadena de custodia y el aseguramiento de prueba sin embargo ha terminado siendo una oportunidad desperdiciada. Para tratar de suplir de algún modo este vacío legislativo la jurisprudencia ha dado directrices para resolver algunos de los problemas plantead. Esto no deja de ser, a mi juicio, una solución provisional ya que la regulación legal sigue siendo necesaria y, esperemos, que en los próximos años se puedan llegar a corregir estas carencias.

---

incautados no habían sido clasificados en función del domicilio en el que se habían recogido. Además el perito recibió los CD-ROM en contenedores rotos y sin etiquetar y siendo estos un número superior al incautado según lo que constaba en las diligencias. Ante esto el Tribunal afirma que no se ha respetado la cadena de custodia del siguiente modo: "Ello acredita que se ha producido una deficiente custodia policial y control judicial de dicho material, que no estaba debidamente precintado y a salvo de eventuales manipulaciones externas tanto de carácter cuantitativo (número de las piezas de convicción halladas en los registros) como cualitativo (contenido de aquellos soportes que admitieran una manipulación por su carácter regrabable o simplemente por su
naturaleza virgen en el momento de su incautación, e incluso su sustitución por otros), lo que impide que pueda afirmarse que la incorporación al proceso penal de los soportes informáticos se diera con el cumplimiento de las exigencias necesarias para garantizar una identidad plena e integridad en su contenido con lo intervenido y, consecuentemente, que los resultados de las pruebas periciales se realizaran sobre los mismos soportes intervenidos o que éstos no hubieran podido ser manipulados en cuanto a su contenido."

5. CONCLUSIONES

PRIMERA

Las nuevas tecnologías no solo han traído el desarrollo de nuevos dispositivos electrónicos, novedosos avances informáticos o la creación de una red de comunicación mundial, también han surgido nuevas formas de criminalidad, fenómeno que conocemos como cibercrimen

SEGUNDA

La práctica de diligencias realiza por los cuerpos de seguridad debe ajustarse a las peculiaridades de la ciberdelincuencia y por ello ha sido necesario crear unidades especializadas en esta materia compuestas por agentes con una formación concreta y avanzada en las nuevas tecnologías. A nivel nacional, destaca la BIT como unidad destinada a combatir el cibercrimen mientras que a nivel europeo el EC3 es el organismo análogo.

TERCERA

La necesidad de regulación legal ha traído consigo la promulgación de la LO 13/2015 siendo la primera en recoger el acceso remoto a los equipos informáticos como diligencia de investigación. Aunque se trate de un gran avance aún se generan grandes dudas acerca de esta figura que deberían ser resultas mediante reformas del texto legal lo antes posible.

CUARTA

Una de las formas de llevar a cabo el acceso remoto es mediante el uso de virus espía, esto es: de alojar programas informáticos en un determinado dispositivo y capturar la información que entre y salga de él por medio de una red de datos. Sería necesaria una actualización del texto legal, incluyendo una tipología de los tipos de spywares que se permite emplear para delimitar el alcance de las intromisiones permitido.

QUINTA

Otra de las reformas que propuestas desde este trabajo vendría enfocada a corregir la amplitud de alguno de los preceptos, en concreto aquel que impone deber de colaboración a nivel de técnicas de hacheo (entre otras) “a cualquier persona”.

SEXTA

la ley se encarga también de delimitar ante que delitos puede emplearse este tipo de diligencias sin embargo vuelve en esta ocasión a configurar la lista de forma excesivamente abierta al incluir todos los "Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación".

SÉPTIMA

Debería corregirse la excesiva amplitud de los preceptos no solo por la consecuente inseguridad jurídica e injerencia en el principio de legalidad, si no qué esto permite la aplicación de diligencias con un gran alcance invasivo para la defensa de intereses que quizás no superasen un juicio de ponderación. Entre estos intereses revisten una importancia capital los Derechos Fundamentales de los investigados.

OCTAVA

Para que la diligencia sea legal deberán concurrir los siguientes requisitos: la existencia de un fundamento legal para proceder de ese modo que exista proporcionalidad y necesidad en el uso de la medida y que mediante su uso no se afecte al contenido esencial del derecho fundamental en cuestión.

NOVENA

El acceso remoto, llevado a cabo mediante la actuación policial especializada, deberá respetar los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad en sus indagaciones y no podrá sobrepasar los límites configurados legalmente. Si no se respetan estos extremos cualquier prueba obtenida adolecerá de nulidad.

DÉCIMA

Las características de la prueba electrónica suponen adaptar el proceso de la cadena de custodia tradicional. A pesar de que en la práctica se tomen ciertas cautelas como el clonado de los datos, la utilización de algoritmos hash para asegurar la identidad de lo estudiado con el material original o la fe pública del letrado de la administración de justicia no existe un protocolo de actuación regulado en la ley.

UNDÉCIMA

La ausencia de protocolos regulados nuevamente nos coloca ante una importante laguna legal y con la inseguridad jurídica que esta conlleva.

ANEXO

PROPUESTA PARA UN PROTOCOLO DE CADENA DE CUSTODIA

Como se ha reflejado en el último punto de este trabajo existen protocolos establecidos en la ley sin embargo sería fundamental contar con un procedimiento reglado y reconocido en un texto legal a fin de unificar la cadena de custodia, evitar inseguridad jurídica, reforzar las garantías de los investigados y suprimir posibles arbitrariedades.

Mediante el establecimiento de este protocolo se trataría de garantizar que el material recogido y el objeto de examen pericial es el mismo de modo que las evidencias presentadas al juez y que gocen de inmediación sean las mismas que las encontradas en la escena del crimen

Las dos cautelas que VELASCO NUÑEZ presenta a mi juicio deberían ser incluidas en este protocolo, combinadas con otras pautas señaladas por otros autores, a continuación presento mi propuesta combinando las aportaciones de los autores que más interesantes me han parecido con medidas que aporto conforme a mi propio criterio basado en el estudio de esta materia.

En primer lugar sería indispensable que el momento de la recogida contase con las mismas cautelas que las pruebas de naturaleza tradicional, esto es presencia de fedatario público y correcto almacenamiento hasta su examen. De forma que el contenedor en el que fuera depositada la misma garantizase que el aislamiento manteniéndose precintado hasta la pericia. En primer lugar, antes de la pericia y de realizar las dos copias de las que hablábamos, deberá obtenerse el algoritmo hash a fin de comparar después los resultados para garantizar identidad entre las evidencias.

A continuación y cuando nos encontremos ante datos obtenidos mediante registro remoto deberán hacerse dos copias (además de la información original obtenida que se almacenará en el quipo empleado para el acceso remoto) y ambas en formato no modificable. En la primera el volcado de los datos se produciría sobre equipo o disco duro sobre el cual vaya a practicar el perito su examen y otra copia idéntica deberá conservarse en el soporte adecuado (como un disco duro) custodiado por letrado de la administración de justicia en el juzgado.

Concretar los omentos en que sería indispensable la presencia del fedatario público es un punto clave de este protocolo. A mi juicio estos deberían ser el momento de la recogida de las evidencias, la obtención de la clave alfanumérica mediante algoritmos hash (clave que también deberá custodiar el letrado de la administración de justicia) realización del volcado de los datos y desprecito del dispositivo donde se encuentre la evidencia original y de la copia custodiada para comparar las claves después del examen. En caso d que el procedimiento fuera puramente informático no sería necesaria la presencia del fedatario durante su tramitación sin embargo si

consistiese en la visualización de imágenes o videos o lectura de documentos si deberá presenciarlo y dar fe de lo visto.

La propuesta de adopción de un protocolo esencial hecha por CUADRADO SALINAS en mi opinión sería una gran medida adoptar. Los datos más relevantes a incluirse en el mismo serían una cronología de la cadena de custodia, apuntando cada contacto con el material probatorio y quien lo realiza, en el orden en que se produce así como los datos de identificación de todo aquel que entre en contacto con la prueba.

Una opción a considerar seria grabar el proceso del examen pericial. Al igual que las vistas judiciales se graban para su posterior visualización en caso de que este sea necesario, los exámenes periciales también debería hacerse para una mayor obtención de garantías al respecto. Al igual que en el caso de los juicios esto puede ser clave de cara a una segunda instancia la grabación del examen pericial podría ser vital para una eventual pericia contradictoria. El gasto económico sería asumible puesto que el volumen de grabado resultaría enormemente inferior al obtenido mediante el registro audiovisual de las vistas y el gasto temporal tampoco supondría un problema ya que solo se procedería al examen de las cintas en caso de la prueba de identidad de los algoritmos hash no fuese satisfactoria.

Por último, durante el examen pericial deberían seguirse para su realización el mismo tipo de procedimiento en los casos que guarden identidad. Es decir, utilizar métodos informáticos, redactados por profesionales en la materia, previamente reglados y plasmados en un soporte para evitar arbitrariedades y en qué caso de que se produzca algún error que sea más fácil localizarlo entre los pasos de proceso.

BIBLIOGRAFÍA

AGUILAR, M. M. (2015). Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. *Revista Criminalidad*, 57 (1), págs. 121-135.

ALVAREZ SERNA, A., MARTIN RIVERA, O.D., VICTORIA MORALES J.D., "Framework para la computación forense en Colombia". Nº2, *USBMed,* 2012, pág. 67.

AMÉRIGO SÁNCHEZ J.L., "El régimen jurídico del malware según la Ley de Propiedad Intelectual" Nº 8436, *Diario La Ley,* 2014, Pág.4.

BONILLA CORREA. J.A., "Los avances tecnológicos y sus incidencias en la ejecución de la diligencia de registro en domicilio", Nº 8522, *Diario La Ley*, 2015, Pág. 11.

BUENO DE MATA, F., "Prueba electrónica y proceso 2.0. Especial referencia al proceso civil", *Tirant lo Blanch,* 2014, Pág. 14.

BUENO DE MATA. F., "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica" Nº 8627, *Diario La Ley*, 2015, Pág. 1-8.

CUADRADO SALINAS, C. "Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa", Nº 107, *Editorial LA LEY,* 2014, Pág.7-8.

DAVARA RODRÍGUEZ, M.A., "Las videncias electrónicas", Nº 20, *Editorial LA LEY,* 201,1 pág. 24-28.

DE LA CORTE IBÁÑEZ. L, BLANCO NAVARRO. J.M., "seguridad nacional amenazas y respuesta" *LID editorial,* 2014, pág. 20.

DOLZ LAGO M.J., "Child grooming y sexting: anglicismos, sexo y menores en el Código Penal tras la reforma del 2015", Nº 8758, *Diario La Ley*, 2016, Pág. 4-9.

EIRANOVA ENCINAS, E., "Cadena de Custodia y Prueba de Cargo", Nº 6863, *Diario La Ley,* 2008, Pág.4.

FERNÁNDEZ TERUELO, J., "Cibercrimen. Los delitos cometidos a través de internet", *Constitutio Criminalis Carolina*, 2007, pág. 13.

GONZÁLEZ RUS, J.J., "La criminalidad organizada en el Código Penal español. Propuesta de reforma". núm. 30, *Anales de Derecho*, 2012, pág. 25.

LOPEZ, A. "La investigación policial en Internet: estructuras de cooperación internacional* Monográfico III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas", nº5 *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, 2007, PÁG. 69.

ORTIZ PRADILLO, J.C., "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica" en "El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito", edición nº 1, *Editorial LA LEY*, 2012. Pág. 3.

ORTIZ PRADILLO, J.C., "El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito" ,nº 1, *Editorial LA LEY*, 2012, Pág. 5.

RICHARD GONZÁLEZ, M., "Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización", Nº 8808, *Diario La Ley*, 2016, Pág. 15.

RIVERO J., 2008-2009 Entrevista a Manuel Vázquez López Comisario Jefe de la Brigada de Investigación Tecnológica de la Policía, *nº28, a+*, pág. 33-38.

RODRÍGUEZ LAINZ, J.L., "¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?", Nº 8729, Editorial LA LEY, 2016, Pág. 7.

RUBIO ALAMILLO, J., "La informática en la reforma de la Ley de Enjuiciamiento Crimina", No 8662, *Diario La Ley*, 2015, pág. 9.

SANCHEZ BRAVO, A.A., "El convenio del Consejo de Europa sobre cibercrimen: control vs. libertades públicas", No 5528, *Diario La Ley*, 2002, pág. 18.

SANZ-GADEA GÓMEZ, J.B., "Los informes periciales informáticos en el ámbito de las nuevas tecnologías y prueba ilícita" Nº39, *Revista Jurídica de Canarias*,2015, pág. 69-70.

VELASCO NÚÑEZ E., "Delitos informáticos realizados en actuación organizada", Nº 7743, *Diario La Ley,* 2011, Págs. 1 y 2.

VELASCO NUÑEZ, E., "ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal" Nº 82, *Editorial LA LEY,* 2011, Pág. 2-6.

VELASCO NÚÑEZ, E., "Diligencias de investigación penal" en "Delitos cometidos a través de internet", edición nº 1, *Editorial LA LEY,* pág 34-44.

VELASCO NÚÑEZ.E, "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías" número 4, *Revista de Jurisprudencia,* 2011. Pág.2.

VIDE LUEHR, P.H., "Real Evidence, Virtual Crimes. The role of Computer Forensic Expert", N.o 20, *Criminal Justice,* 2005- 2006, p. 17.

ÍNDICE DE JURISPRUDENICA