ESCVELA DE PRÁCTiCA JVRíDiCA
SALAMANCA

TRABAJO FIN DE TÍTULO

MÁSTER EN ACCESO A LA ABOGACÍA

Curso 2015/2017

LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA Y SU APLICACIÓN PRÁCTICA EN EL ORDEN JURISDICCIONAL PENAL

Nombre de la alumna: Laura Valdivielso Villanueva

Tutor: Don Federico Bueno de Mata

Diciembre de 2016

TRABAJO FIN DE TÍTULO

MÁSTER EN ACCESO A LA ABOGACÍA

LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA Y SU APLICACIÓN PRÁCTICA EN EL ORDEN JURISDICCIONAL PENAL

THE TECHNOLOGICAL RESEARCH AND ITS IMPLEMENTATION IN THE CRIMINAL JURISDICTIONAL ORDER

Nombre del estudiante: Laura Valdivielso Villanueva
e-mail: laura_valdi@hotmail.com

Tutor: Federico Bueno de Mata

RESUMEN

La práctica por parte de las Fuerzas y Cuerpos de Seguridad del Estado de determinadas diligencias de investigación, caracterizadas por una completa ausencia de regulación legal, ha dado lugar a numerosos pronunciamientos mediante los cuales nuestros Tribunales han tratado de hacer frente a dicha laguna jurídica, debido a la injerencia que dichas prácticas provocan sobre derechos fundamentales tan importantes como el derecho al secreto de las comunicaciones o el derecho a la intimidad.

Presentada como un instrumento para el fortalecimiento de las garantías procesales, la LO 13/2015, de 5 de octubre, también se ocupa de poner fin al vacío normativo existente en torno a las diligencias de investigación tecnológicas, centrándose en los requisitos que deben cumplir la resolución judicial habilitante de cada una de ellas, limitando su ámbito objetivo de aplicación, y muchos otros aspectos como su duración.

Estas diligencias cobran un especial papel en el orden jurisdiccional penal, debido al incremento, tanto de los tipos como de los casos, que día a día se comenten de delitos informáticos, siendo una pieza fundamental en la fase probatoria de los mismos al constituir la principal fuente de obtención de las pruebas electrónicas que los hacen frente.

PALABRAS CLAVE: Diligencias investigación, prueba electrónica, delitos informáticos.

ABSTRACT

The practice by the State Security Forces of certain investigations, characterized by a complete lack of legal regulation, has led to numerous pronouncements by which our Courts have tried to deal with this legal loophole, because the interference that these practices give rise to fundamental rights as important as the right to secrecy of communications or the right to privacy.

Presented as an instrument for the strengthening of procedural safeguards, LO 13/2015, of October 5, also deals with putting an end to the existing regulatory vacuum regarding technological research, focusing on the requirements that must be met Judicial decision authorizing each of them, limiting its scope of application, and many other aspects such as its duration.

These proceedings have a special role in the criminal jurisdictional order, because to the increase in both types and cases, which are discussed day by day of cybercrime, being a key element in the probationary phase of the same as the main Source of obtaining the electronic evidence that faces them.

KEYWORDS: Investigations, electronic evidence, cybercrimes.

ABREVIATURAS

AN	Audiencia Nacional
AP	Audiencia Provincial
ARP	Aranzadi Penal
Art.	Artículo
AS	Aranzadi Social
BIB	Bibligrafía
CD-ROM	Compact Disc Read-Only Memory (Disco Compacto de Solo Lectura)
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
CP	Código Penal
DVD	Digital Versatile Disc (Disco Versátil Digital)
DNS	Domain Name System (Sistema de Nombres de Dominio)
FJ	Fundamento Jurídico
GPS	Global Positioning System (Sistema de Posicionamiento Global)
IMEI	International Mobile Station Equipment Identity (Identidad internacional de equipo móvil)
IMSI	International Mobile Subscriber Identity (Identidad Internacional del Abonado a un Móvil)
IP	Internet Protocol (Protocolo de Internet)
ISBN	International Standard Book Number (Número Internacional Normalizado del Libro).
ISSN	International Standard Serial Number (Número Internacional Normalizado de Publicaciones Seriadas)

JP	Juzgado de lo Penal
JUR	Resoluciones no publicadas en los productos CD/DVD de Aranzadi
LEC	Ley de Enjuiciamiento Civil
LECrim.	Ley de Enjuiciamiento Criminal
LO	Ley Orgánica
LOGP	Ley Orgánica General Penitenciaria
Núm. /Nº	Número
NJ	Noticias Jurídicas
Pág. /Págs.	Página/Páginas
RD	Real Decreto
RDLey	Real Decreto Ley
RJ	Repertorio de Jurisprudencia Aranzadi
RTC	Repertorio Aranzadi del Tribunal Constitucional
SITEL	Sistema Integrado de Interceptación Telefónica
SMS	Short Message Service (Servicio de mensajes cortos)
TEDH	Tribunal Europeo de Derechos Humanos
Tco.	Tribunal Constitucional
TIC's	Tecnologías de la Información y la Comunicación
TPV	Terminal Punto de Venta
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia

ÍNDICE

I. INTRODUCCIÓN

Las nuevas tecnologías han influido a lo largo de los años en múltiples ámbitos presentes en nuestra vida cotidiana. Desde el modo en el que nos transportamos, la obtención de una comunicación más rápida y eficaz mediante la creación del correo electrónico o el ya conocido "Whatsapp" encargado de proveer mensajería, llamadas por Internet y otros servicios alrededor del mundo, la forma de relacionarnos con los demás con el surgimiento de distintas redes sociales tales como "Facebook" o "Twitter", pasando por el mundo laboral, hasta la manera en la que obtenemos información del mundo exterior o adquirimos conocimientos, entre otros.

El impacto social que todas ellas han provocado resulta innegable, al igual que las infinitas ventajas que llevan aparejadas. Sin embargo, no podemos obviar los inconvenientes e incluso peligros que van unidos a un mal uso de las mismas.

Un mundo en el que las nuevas tecnologías no han pasado desapercibidas por podernos afectar a todos y cada uno de los ciudadanos de una manera u otra es el mundo jurídico. Ejemplos de este suceso los encontramos con la llegada de los primeros ordenadores a la administración pública española en la década de los años 60, la aparición de los primeros ficheros automatizados o la entrada en vigor de diversas normas jurídicas en las que ya se hacía referencia a los avances experimentados, pudiendo citar como origen la LO 16/1994, de 8 de noviembre, por la que se reforma la LO 6/1985, de 1 de julio, del Poder Judicial, y posteriormente el RD 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, la regulación completa de la firma electrónica a través del RDLey 14/1999, de 17 de septiembre, o la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, encargada de regular entre otros el expediente judicial electrónico y la sede judicial electrónica.

Todas estas novedades tienen como objetivo principal modernizar nuestro sistema judicial, logrando así una justicia más rápida y eficiente tratando de acabar con las indebidas dilaciones temporales a las que se someten los ciudadanos para obtenerla.

Dejando a un lado la cara positiva que presentan las nuevas tecnologías, la ya mencionada inclusión de éstas en nuestras vidas cotidianas también ha llevado consigo la aparición de nuevas formas de delincuencia en el orden penal ligadas al uso de las nuevas tecnologías. Estos delitos informáticos o ciberdelitos, los cuáles serán desarrollados en el presente trabajo, se cometen día tras día y es por ello, que han dado lugar a nuevas formas de llevar a cabo la investigación de los mismos por medio de nuevas medidas de investigación tecnológicas mediante la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Esta norma además

de llevar a cabo modificaciones en lo relativo a la detención y apertura de la correspondencia escrita y telegráfica, es de principal interés en el presente trabajo, analizar las nuevas diligencias de investigación tecnológica recogidas en la misma centrándonos en sus presupuestos, requisitos, duración, metodología, cuestiones prácticas, etc. Así mismo, se llevará a cabo un análisis jurisprudencial de las mencionadas diligencias con el objetivo de conocer cómo nuestros Tribunales han suplido la laguna judicial existente en torno a ellas, y los criterios establecidos para configurar una práctica de las mismas lo más segura y proporcional posible.

Junto a las nuevas formas de delincuencia, el empleo de forma exclusiva en la comisión de delitos, tanto informáticos como tradicionales, de las nuevas tecnologías hace que muchas veces, las partes en un proceso judicial únicamente puedan presentar como prueba de los hechos alguno de los elementos ya mencionados como correos electrónicos, SMS, capturas de Whatsapp, USB, etc., obtenidos en muchas ocasiones gracias a la investigación penal llevada a cabo por la Policía Judicial empleando algunas de las diligencias anteriormente mencionadas.

Estos nuevos materiales probatorios nacidos del avance tecnológico, han pasado a conocerse en su conjunto como "prueba electrónica" y debido al protagonismo que está teniendo ésta en muchos de los procesos judiciales que se tramitan a diario en nuestro país, el presente trabajo también se centrará en poder ofrecer una conceptualización de la misma, tratando de fijar su naturaleza y tipología, así como de juntar toda la regulación que hay en torno a ella a pesar de ser dispersa y escasa como veremos más adelante.

En cuanto a la metodología seguida para la realización del presente trabajo, una vez llevada a cabo la elección del tema por su actualidad, aplicación práctica e interés personal, y tras la decisión de darle una perspectiva nacional a mi estudio, comencé con la búsqueda, recopilación y lectura de monografías idóneas facilitadas por la Biblioteca Francisco de Vitoria, artículos publicados en diferentes revistas mediante el portal bibliográfico Dialnet, así como Aranzadi y artículos relevantes extraídos de Internet.

Todos ellos me han ayudado no sólo a sentar las bases y contenidos específicos de cada uno de los apartados de éste trabajo, sino a conocer cuáles han sido las principales resoluciones judiciales dictadas en cada uno de ellos.

Por lo que se refiere al trabajo con las sentencias, una vez conocidas cuál eran las más destacables, la metodología ha consistido en su búsqueda a través de Aranzadi Digital, procediendo posteriormente a su lectura, haciendo especial hincapié en los fundamentos jurídicos encargados de resolver la cuestión controvertida que fuera de interés en cada caso, ya que, en muchas ocasiones, el fallo de la misma no se correspondía con lo resuelto en ellos. Además, tanto la búsqueda por "voces", como la opción "sentencias a favor" presente en cada una de las resoluciones, me han permitido conocer otros veredictos no hallados en las diferentes monografías y artículos, pudiendo conocer supuestos y argumentos distintos.

II. LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA SEGÚN LA LO 13/2015

Como ya avanzaba en la Introducción, existe una innegable vertiente negativa derivada del uso inadecuado de las nuevas tecnologías. Sin embargo, un buen empleo de las mismas puede ayudar a las Fuerzas y Cuerpos de Seguridad del Estado en la investigación y persecución de diversas conductas delictivas.

Entre los objetivos fijados en la pasada legislatura, encontramos la elaboración de un nuevo Código Procesal Penal; sin embargo, éste nunca llego a la mesa del Consejo de Ministros[1]. Viendo que esta norma no llegaba y ante la imposibilidad de esperar a su promulgación, el 6 de diciembre de 2015 entró en vigor la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, encargado de trasponer la Directiva 2013/48/UE del Parlamento Europeo.

Con esta reforma de la LECrim, al fin se concede a diversas diligencias de investigación tecnológica la regulación que desde hace años se venía demandado, mediante la introducción en su Título VIII los nuevos capítulos V, VI, VII, VIII, IX y X.

Diversos pronunciamientos del TEDH[2] acerca de la carente legislación española en esta materia, la incidencia de dichas diligencias en derechos fundamentales tan importantes como la intimidad, el secreto de las comunicaciones o la inviolabilidad del domicilio[3], unido al uso cada vez más frecuente e imprescindible para la instrucción de algunos delitos como los analizados en el punto anterior, hacen que su ordenación se calificara como necesaria y urgente.

Es por ello que, además de establecer una serie de disposiciones comunes, la LO 13/2015 fija una regulación específica para cada una de las siguientes diligencias de investigación tecnológica, haciendo un resumen a continuación.

[1] MUERZA ESPARZA, Julio. La reforma procesal penal de 2015. *Aranzadi digital parte Estudios y comentarios*. 2015, Nº 1 (BIB 2015\16990).

[2] Por ejemplo en el caso *Abdulkadir Cobán vs España*, donde el TEDH pone de manifiesto el deseo de una modificación legislativa que incorpore a la Ley los principios que se desprenden de la jurisprudencia del Tribunal, todo ello en su Decisión de 26 de Septiembre de 2006 (TEDH 2006\5).

[3] En palabras de la **STCo. 22 septiembre 2014 (RTC 2014/145)**, y plasmado en su FJ Séptimo, "por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, que incida directamente sobre su desarrollo o limite o condicione su ejercicio, precisa, además, una habilitación legal".

1. La interceptación de las comunicaciones telefónicas y telemáticas (Art. 588 ter a. – Art. 588 ter m.)

Esta diligencia únicamente podrá autorizarse cuando su objetivo sea la investigación de alguno de los delitos recogidos en el artículo 579.1 de la LECrim[4], o cuando se trate de delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación, o servicios de comunicación.

Únicamente podrá afectar a terminales o medios de comunicación empleados habitual y ocasionalmente por la persona investigada de los que sea titular o usuario, al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados[5] al proceso de comunicación, o los producidos en una comunicación en la que participe el sujeto investigado independientemente del establecimiento o no de una comunicación. Excepcionalmente, y refiriéndonos al sujeto sobre el que recae la diligencia, también podrá afectar a las comunicaciones de la víctima si se prevé un riesgo para su vida o integridad, y a los terminales de una tercera persona cuando esté colaborando con el investigado o éste le utilice para transmitir o recibir información.

Para poder establecer la referida interceptación es necesario solicitar previamente una autorización judicial, haciendo constar en ella obligatoriamente la identificación del número de abonado, del terminal o de la etiqueta técnica y una de estas dos opciones: o la identificación de la conexión objeto de la intervención o los datos necesarios para identificar el medio de telecomunicación de que se trate. Junto a estos extremos, también se deben incluir los ocho puntos contenidos en el artículo 588 bis b[6], comunes para todas las solicitudes de diligencias. También se requerirá autorización judicial para poder obtener aquellos datos electrónicos operativos en archivos automatizados y conservados por los prestadores de servicio o personas que faciliten la comunicación, siempre y cuando estén vinculados al proceso de comunicación y resulten imprescindibles para la investigación.

Una vez se ha obtenido la autorización judicial, solo se podrá extender en el tiempo durante tres meses, aunque existe la posibilidad de prorrogarla siempre y cuando se

[4] Estos son tres: delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión**;** delitos cometidos en el seno de un grupo u organización criminal; delitos de terrorismo.

[5] Son todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga (Art. 588 ter b.).

[6] **1.º** La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos. **2.º** La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia. **3.º** Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida. **4.º** La extensión de la medida con especificación de su contenido. **5.º** La unidad investigadora de la Policía Judicial que se hará cargo de la intervención. **6.º** La forma de ejecución de la medida. **7.º** La duración de la medida que se solicita. **8.º** El sujeto obligado que llevará a cabo la medida, en caso de conocerse.

fundamente por la Policía Judicial por periodos de otros tres meses hasta un plazo máximo de dieciocho meses.

En las labores de investigación mediante interceptación de comunicaciones, es posible que la Policía Judicial no se encuentre sola, contando con la colaboración de los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones y en general los mencionados en el artículo 588 ter e., siempre y cuando requieran de su asistencia. En caso de no prestarla, podrán incurrir en un delito de desobediencia.

Así mismo, en este capítulo se concretan tres instrumentos, de los que puede valerse la Policía Judicial para poder identificar a usuarios, terminales y otros dispositivos de conectividad: la dirección IP[7], la numeración IMSI[8] o IMEI[9]. En relación con estos términos se debe destacar la Circular 1/2013, de la Fiscalía General del Estado, sobre pautas en relación con la dirigencia de la intervención de las comunicaciones telefónicas, por recoger los conceptos de cada uno de ellos, su naturaleza e incluso diversa jurisprudencia dictada en torno a los mismos.

Finalmente, se recoge un supuesto inusual por no requerirse autorización judicial para su instauración. Éste se identifica con casos urgentes, debiéndose cumplir cuatro requisitos: que tenga como finalidad la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas, que la medida sea imprescindible, que la ordene a el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad y que se comunique al juez con la mayor inmediatez posible y, en todo caso, dentro del plazo máximo de veinticuatro horas. El juez podrá fin a la misma o decidirá su continuación en las setenta y dos horas siguientes desde su ordenación.

Dejando a un lado el plano teórico, en la actualidad para la intervención de las telecomunicaciones se emplea el sistema SITEL[10], llevando a cabo la interceptación de una manera automatizada en el servidor central, pasando posteriormente la grabación a un

[7] La dirección IP es un número único e identificativo que se le asigna a tu equipo para identificarlo de forma inequívoca cuando éste se conecta a una red. Algo así como la matrícula de tu coche o tu DNI. Vía: Rubén Andrés. *Cómo saber cuál es la dirección IP de mi ordenador*. (http://computerhoy.com/paso-a-paso/internet/como-saber-cual-es-direccion-ip-mi-ordenador-24347). [Fecha de consulta: 20-10-2016].

[8] Definido en la **STS 20 mayo 2008 (RJ 2008/4387)** como un código de identificación único para cada dispositivo de telefonía móvil, representado por una serie de algoritmos, que se integra en la tarjeta SIM y que permite su identificación a través de las redes GSM y UMTS. Mediante su tratamiento automatizado y su interrelación con otros datos en poder del operador puede llegar a obtenerse, entre otros datos, la identidad del comunicante.

[9] Código pregrabado en cada terminal y su función principal es identificar a los móviles a nivel mundial. Vía: PALMA, Antonio. *Cómo conocer el código IMEI de mi móvil.* (http://tecnologia.uncomo.com/articulo/como-conocer-el-codigo-imei-de-mi-movil-18353.html). [Fecha de consulta: 20-10-2016].

[10] Consistente en un avanzado sistema informático desarrollado por la multinacional Ericsson en el año 2002, depende del Ministerio del Interior y es utilizado conjuntamente por las Direcciones Generales de Policía y Guardia Civil (DGPGC), así como por el Centro Nacional de Inteligencia (CNI). Este sistema no se limita, única y exclusivamente a la interceptación de las conversaciones telefónicas, sino que también interviene los datos electrónicos de tráfico o asociados el SITEL. Vía: VIDAL MARÍN, Tomás. RUIZ DORADO, María. Análisis de la constitucionalidad del SITEL. Breves consideraciones a partir de la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal. *Revista Aranzadi Doctrinal.* 2016, Nº 9. ISSN:1889-4380.

DVD, siendo éste el que finalmente se aporta al Juzgado.

2. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (Art. 588 quater a. – Art. 588 quater e.)

Con la regulación de esta medida, se permite la captación y grabación de comunicaciones orales directas y previsibles, en las que intervenga el investigado junto a terceras personas, pero nunca en las que éste se encuentre ausente, pudiendo emplear todo tipo de dispositivos técnicos, y completar la información obtenida mediante la captación de imágenes, siempre y cuando conste de manera expresa en la autorización emitida por el juez habilitante de la diligencia.

Los instrumentos empleados no sólo podrán instalarse en la vía pública o cualquier otro espacio abierto, sino también en el domicilio del investigado (tanto en el interior como en el exterior del mismo) o en cualquier otro lugar cerrado. Ello supone una mayor intromisión en su privacidad, por lo que será necesario que la resolución habilitante justifique a su vez la imperiosa necesidad de entrada en el domicilio, debiendo ser esta lo más discreta posible.

Al igual que la diligencia anterior, la grabación de comunicaciones orales también encuentra limitado su ámbito de aplicación ya que únicamente podrá emplearse en la investigación de tres tipos de delitos[11], sobre los que además se prevea aportar datos esenciales y de relevancia probatoria: delitos dolosos castigados con pena de prisión cuyo límite máximo sea al menos de tres años, aquellos cometidos en el seno de un grupo u organización criminal, y también delitos de terrorismo.

Sin embargo, en este caso no se regula de manera especial el contenido de la solicitud previa, sino el de la resolución por la que se autoriza la medida, debiendo concretar tanto el lugar o dependencias, así como los encuentros que van a estar sometidos a vigilancia. A estos dos extremos deberán acompañarles los otros ocho recogidos en el artículo 588 bis c.[12], comunes para todas las diligencias.

Una vez producido el cese de la medida, se solicitará una nueva autorización judicial para la captación de conversaciones que puedan tener lugar en otros encuentros distintos a los autorizados inicialmente.

---

[11] Art. 588 quater b.

[12] **a)** El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida. **b)** La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido. **c)** La extensión de la medida de injerencia, especificando su alcance, así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a. **d)** La unidad investigadora de Policía Judicial que se hará cargo de la intervención. **e)** La duración de la medida. **f)** La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida. **g)** La finalidad perseguida con la medida. **h)** El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

A lo largo de todo el articulado, el legislador se ha limitado a mencionar de manera general la utilización de dispositivos técnicos. Con ello, se concede a los agentes una cierta libertad en torno a la elección del medio adecuado según si la diligencia consiste únicamente en la captación y grabación de comunicaciones orales o, por el contrario, si ésta va acompañada de imágenes. En el primero de los casos, el medio más adecuado se identifica con "la colocación de micrófonos de ambiente que recogen el sonido en su radio de alcance y, a través de diversos dispositivos de emisión y conducción de ese sonido, lo envían a un soporte apto para su grabación y conservación"[13]. Por el contrario, cuando la captación de comunicaciones orales vaya acompañada de imágenes, ambas acciones se llevarán a cabo mediante una grabación de video que recoja ambos datos a la par.

A pesar de que esta diligencia encuentra habilitación legal de una manera reciente, la captación de imagen y sonido a través de grabaciones de vídeo se lleva realizado desde hace años, dando a lugar a diversas controversias. No resultan extraños los casos en los que aseguradoras contratan a detectives privados con la finalidad de demostrar posibles estafas[14]. Sobre este tipo de supuestos se pronunció en 2014 el TEDH[15] a raíz de unas resoluciones dictadas por Tribunales españoles. Alegando el demandante la vulneración del artículo 8 del CEDH al haberse aportado un vídeo, en el proceso de reclamación de indemnización por daños que supuestamente había sufrido en un accidente de tráfico, con el que se demostraba la estafa. El Tribunal Europeo consideró que tal vulneración no existía, ya "que este caso no se refiere a la difusión de imágenes relativas a la vida cotidiana del demandante, sino exclusivamente a la toma y utilización posterior de esas imágenes como medio de prueba en el ámbito de un proceso civil". Además, "tales imágenes no estaban destinadas a ser publicadas, ni su grabación se había efectuado de una manera sistemática o permanente"[16].

---

[13] URIARTE VALIENTE, Luis M. *Nuevas técnicas de investigación restrictivas de derechos fundamentales*. (https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Sr%20Uriarte%20Valiente.pdf?idFile=ec583d09-edd5-4a96-b303-a9fca37cf99e). [Fecha de consulta: 20-11-2016].

[14] En octubre de este año un hombre resultaba condenado por el Tribunal Supremo a tres años y seis meses de prisión por un delito continuado de estafa amputó una mano y simuló un accidente de tráfico para cobrar la indemnización correspondiente a las pólizas que había suscrito con ocho compañías de seguros. Noticia completa en: EFE. *Tres años y medio de cárcel por amputarse una mano para estafar al seguro*. (http://www.rtve.es/noticias/20161014/tres-anos-medio-carcel-amputarse-mano-para-estafar-seguro/1425783.shtml). [Fecha de consulta: 20-11-2016].

[15] **STEDH 27 mayo 2014 (TEDH 2014/34).**

[16] Razonamientos extraídos de: REDACCIÓN NJ. *La grabación realizada en la vía pública y por detectives de la aseguradora, de la víctima de un accidente de tráfico, no vulnera su derecho a la vida privada.* (http://noticias.juridicas.com/actualidad/noticias/3817-la-grabacion-realizada-en-la-via-publica-y-por-detectives-de-la-aseguradora-de-la-victima-de-un-accidente-de-trafico-no-vulnera-su-derecho-a-la-vida-privada/). [Fecha de consulta: 20-11-2016].

3. Utilización de dispositivos técnicos de captación de imagen, de seguimiento y de localización (Art. 588 quinquies a. – Art. 588 quinquies c.)

Refiriéndonos a la captación de imágenes, los sujetos sobre los que puede recaer esta medida comprenden tanto al investigado, como terceras personas siempre y cuando existan indicios de su relación con los hechos o el individuo objeto de investigación. No obstante, y marcando la diferencia con el capítulo anterior, en este caso únicamente se podrán obtener y grabar las imágenes cuando el investigado se encuentre en un lugar o espacio público, sin recoger la opción de su domicilio o un lugar cerrado.

En cuanto a los requisitos, únicamente se requiere que la diligencia sea necesaria para obtener la identificación de la persona investigada, localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos.

En cuanto a los dispositivos técnicos de seguimiento y localización (como las balizas GPS[17]), es necesario que la autorización que los habilite determine de forma específica el medio técnico que se debe emplear. Dicha resolución se concederá siempre y cuando existan razones de necesidad y la medida resulte proporcionada, aunque se puede actuar sin ella cuando concurran razones de urgencia, al igual que en el Capítulo IV. Estos supuestos excepcionales tendrán lugar siempre y cuando se prevea que, de no actuar, la investigación puede fracasar, procediendo la propia Policía Judicial a la instalación de los dispositivos y comunicación a la autoridad judicial en un máximo de 24 horas; mismo intervalo de tiempo en el cual ésta se deberá pronunciar ratificándola o no.

La duración, común en ambas injerencias, está fijada en tres meses, aunque podrá ser prorrogada por el mismo plazo hasta un máximo de dieciocho meses. Una vez finalizada, se deberán entregar al juez los soportes originales o copias electrónicas auténticas que contengan la información recogida.

En la práctica, un instrumento que puede ser empleado en las investigaciones policiales para llevar a cabo tanto las diligencias de captación de imágenes o localización, como las recogidas en el punto anterior, son los drones. Estos aparatos, cuyo uso cada día es más generalizado y multifuncional, desde un punto de vista jurídico son vistos como una "aeronave pilotada por control remoto, o también denominados aviones no tripulados", pudiendo ser empleados "con el fin de instalar una videocámara que permita tomar imágenes en distancia a las que el ojo humano no tiene acceso, o captar sonidos imperceptibles en condiciones normales, incluir sensores de movimientos, sensores de

[17] Consistentes en un "pequeño dispositivo que recibiendo datos de posicionamiento GPS, transmite su localización a otro dispositivo manejado por los agentes investigadores, permitiendo casi con total precisión, hacer un seguimiento minucioso de todos los movimientos del objeto seleccionado, sin más limitaciones que la de la capacidad de la batería que alimente al dispositivo oculto". En la mayoría de casos, son colocadas en coches y embarcaciones. Más sobre este instrumento en: REYES LÓPEZ, Javier Ignacio. Los dispositivos técnicos de geolocalización. Régimen jurídico a partir de la LO 13/2015. *Revista Aranzadi Doctrinal.* 2016, Nº 9. Págs.: 53-66. ISSN: 1889-4380.

temperatura, localizadores, etc."[18]. Entre las principales ventajas que pueden aportar estos dispositivos, podemos destacar una disminución de los riesgos a los que pueden verse expuestos las Fuerzas y Cuerpos de Seguridad a la hora de llevar a cabo la medida, una detección menos probable por parte de los investigados, a la vez que no requieren de una instalación que ponga en peligro la investigación.

A pesar de que en el pasado su uso con estos fines no estaba bien visto por la mayoría de la doctrina ni de la jurisprudencia debido a la ausencia de regulación que los amparara, el articulado actual estudiado anteriormente facilitará su empleo siempre y cuando se cumplan todos los requisitos expuestos, se vea sometido al debido control judicial, y se lleve a cabo bajo los principios de proporcionalidad, necesidad, idoneidad, especialidad y excepcionalidad recogidos en el artículo 588 bis a.

Sin ir más lejos, en la provincia de Salamanca se han creado tres empresas relacionadas con estos dispositivos desde comienzo de año, alcanzando así un total de quince empresas registradas y autorizadas para operar drones de manera profesional. Entre ellas encontramos Giselle Moraes de Passos Severino, destacada por llevar a cabo trabajos de investigación y desarrollo, así como la observación y vigilancia aérea incluyendo filmación y actividades de vigilancia de incendios forestales y publicidad aérea u operaciones de emergencia, búsqueda y salvamento[19]. Por lo tanto, no parece tan remoto ni extraño su aplicación en las investigaciones policiales.

4. Registro de dispositivos de almacenamiento masivo de información (Art. 588 sexies a. – Art. 588 sexies c.)

Normalmente esta diligencia se presenta como consecuencia de un registro domiciliario en el que la policía prevé que en su entrada y registro pueden encontrar ordenadores, móviles, discos duros, etc., con información útil para la investigación. De esta manera, la autorización por la que se habilita a los agentes a entrar en el domicilio y registrar lo allí habido, deberá justificar a su vez el registro de dispositivos masivos de información incluyendo el acceso a repositorios telemáticos de datos.

No obstante, también es posible que el acceso a todos estos dispositivos tenga lugar fuera del domicilio del investigado. En estos casos es necesario que la incautación sea puesta en conocimiento del juez para que autorice el acceso a los datos que pudieran contener. Por lo tanto, la simple incautación no legitima al acceso del contenido[20].

[18] ARIZA CLMENAREJO, María Jesús. La utilización de drones como herramienta en la investigación penal. En: BUENO DE MATA, Federico. *Fodertics 4.0: (estudios sobre nuevas tecnologías y justicia)*. Granada: Comares, 2015. Págs.: 107-116. ISBN: 978-84-9045-274-5. Págs.:107 y 110.

[19] Datos extraídos de: VICENTE DE ANTONIO, Javier. *La moda de los drones arrasa en Salamanca.* (http://www.salamanca24horas.com/local/13-10-2016-alarmante-aumento-de-adicciones-y-ciberacoso-adolescentes-por-internet). [Fecha de consulta: 20-11-2016].

[20] Art. 588 sexies b.

Entre el contenido de la autorización judicial exigida en ambos casos, se podrán observar estos tres extremos[21]:

- Los términos y el alcance del registro.
- Las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible la práctica de un eventual dictamen pericial.
- Puede contener a su vez, una autorización para realizar una copia de los datos informáticos ya que siempre que las circunstancias lo permitan se evitara la incautación de los soportes físicos que contengan los datos y archivos.

Al igual que en las anteriores injerencias, la Policía Judicial podrá actuar sin la habilitación otorgada en la resolución judicial por razones de urgencia que hagan la medida imprescindible, compartiendo en este caso los plazos expuestos en la interceptación de las comunicaciones.

Así mismo se necesitará autorización judicial cuando se desee ampliar el registro inicialmente fijado, al considerar que los datos necesarios están almacenados en otro sistema informático o en una parte de él, siempre y cuando se puedan contener de manera licita por el sistema inicial. Esta ampliación también puede llevarse a cabo sin contar con el visto bueno del juez cuando se esté ante un supuesto de urgencia.

Toda persona que pueda ayudar de una manera u otra, a los agentes que tengan encarga esta tarea, deberá prestar su colaboración bajo aviso de incurrir en un delito de desobediencia.

5. Registros remotos sobre equipos informáticos (Art. 588 septies a. – Art. 588 septies c.)

Cuando la Policía Judicial cuente con autorización judicial para la realización de esta diligencia, el registro podrá recaer sobre ordenadores, dispositivos electrónicos, un sistema informático, instrumentos de almacenamiento masivo de datos o sobre base de datos. Sin embargo, y a diferencia de la injerencia anteriormente expuesta, en estos supuestos no se producirá una incautación física y posterior registro, sino que éste tendrá lugar de forma remota y telemática, al haber obtenido los datos de identificación y códigos o mediante la instalación de un software que permita el rastreo.

A pesar de que su ámbito de aplicación también se encuentra limitado, podemos encontrar un catálogo de delitos más amplio[22]:

- Delitos cometidos en el seno de organizaciones criminales

[21] Art. 588 sexies c.
[22] Art. 588 septies a.

- Delitos de terrorismo
- Delitos cometidos contra menores o personas con capacidad modificada judicialmente
- Delitos contra la constitución, de traición y relativos a la defensa nacional
- Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

La resolución judicial emitida para este tipo de registros debe detallar cinco aspectos: el objetivo sobre el que recae la medida, el alcance y la forma en la que se va a acceder a los datos especificando el software a emplear, los agente autorizados para realizarlo, la habilitación para realizar y conservar las copias de los datos obtenidos, y las medidas para la preservación de la integridad de los datos y para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

Al igual que en el registro del capítulo anterior, se podrá autorizar una ampliación de los términos del registro cuando existan razones suficientes, y se impone un deber de colaboración a aquellas personas que conozcan el funcionamiento del sistema informático o las medidas a aplicar para proteger los datos informáticos contenidos en ellos. Sin embargo, este deber no es universal ya que están exentos del mismo el investigado o encausado, las personas que están dispensadas de la obligación de declarar por razón de parentesco, y quienes no pueda declarar en virtud de secreto profesional[23].

Con una duración inferior al resto de diligencias, únicamente se podrá extender durante un mes como máximo y prorrogarse por iguales periodos hasta un máximo de tres meses[24].

Detallada la regulación, un mecanismo que en la práctica puede resultar eficaz para la investigación penal en este tipo de injerencias es el virus troyano o virus espía. En la exposición de los ciberdelitos más comunes que desarrollaré más adelante, veremos sus efectos cuando caen en manos inapropiadas y son empleados con fines ilícitos. Sin embargo, sus características los convierten en idóneos para llevar a cabo los registros remotos, identificándose con el método de "instalación de un software que permita el rastreo".

De esta manera los agentes encargados de la diligencia procederían a la "introducción de software de agente autónomo, previamente programado, que, con imitación de las técnicas de *malware*, mas controladas por los investigadores, busca de

[23] Estas exclusiones también son aplicables al deber de colaboración impuesto en el registro de dispositivos de almacenamiento masivo de información.
[24] Art. 588 septies c.

forma remota datos y comunicaciones internas en el ordenador del sospechoso, copiando lo preseleccionado y enviándoselo a los investigadores para su análisis"[25].

Una vez introducido en el equipo del sujeto investigado, los agentes podrán tener acceso a todos los datos almacenados en el mismo, conocer las comunicaciones que pueda mantener desde medios telemáticos como el correo electrónico, chats, foros, etc, así como los datos almacenados en la famosa "nube" o las páginas webs visitadas por el investigado. Además, la ausencia de una aprehensión física permite que el investigado pueda continuar empleando el equipo informático, pudiendo los agentes seguir sus pasos a medida que va actuando. Una vez toda esa información es duplicada, se remite a los equipos de los investigadores para su posterior examen y análisis.

Su uso se ha ido extendiendo a lo largo de los años; Estados Unidos fue el primer país en emplear y aprobar este tipo de programas para destinarlos a la investigación de equipos, en Europa la iniciativa la protagonizó Alemania al configurarla como una medida excepcional de investigación únicamente de delitos relacionados con el terrorismo internacional[26], y en España con la regulación conferida por la LO 13/2015, de 5 de octubre, se espera que su uso se vaya generalizando al contar ya con la exigida habilitación legal y la gran utilidad que puede representar en investigaciones policiales relativas a ciberdelitos.

6. El agente encubierto en Internet

Hasta la reforma experimentada por la Ley de Enjuiciamiento Civil, la figura del agente encubierto únicamente se encontraba regulada en su faceta física, concretamente por vía del artículo 282 bis LECrim.

Con la entrada en vigor de la LO 13/2015, en el referido artículo se añaden dos apartados más, los apartados 6 y 7, con la finalidad de introducir en nuestro texto legal el agente encubierto informático, al que se le aplicarán las mismas condiciones fijadas para el agente encubierto tradicional.

En primer lugar, para que esta práctica pueda llegar a producirse es necesario que exista una autorización, bien otorgada por el Juez de Instrucción, bien por el Ministerio Fiscal dando cuenta inmediata al Juez, en la que se recoja tanto el nombre verdadero del agente que va a llevar a cabo la infiltración, como la identidad falsa con la que actuará. El encargado de concederle dicha identidad será el Ministerio del Interior y será válida durante

[25] CAMPANER MUÑOZ, Jaime. ¿*Remore Forensic Software* en España? Acerca de la utilización de virus con fines de investigación en el proceso penal. En: BUENO DE MATA, Federico. *Fodertics II: hacia una justicia 2.0.* Salamanca: Ratio Legis, D.L. 2014. Págs.: 107-112. ISBN: 978-84-9045-274-5. Pág.:108.

[26] ORTIZ PRADILLO, Juan Carlos. Hacking legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática. En: *Delincuencia informática. Tiempos de cautela y amparo.* Cizur Menor (Navarra): Thomson Reuters Aranzadi, 2012. Págs.: 177-220. ISBN: 978-84-9014-273-8. Pág.: 194.

seis meses, pudiendo prorrogarse por periodos de igual duración. Así mismo, se requerirá autorización judicial cuando, estando vigente esta medida, alguna de las actuaciones que tengan lugar en ella puedan afectar a los derechos fundamentales.

Refiriéndonos ahora al ámbito en el que podrán tener lugar las infiltraciones, éste viene limitado por tres exigencias. En primer lugar, es necesario que la investigación este orientada hacia actividades propias de la delincuencia organizada[27]. En segundo lugar, la investigación debe estar orientada a esclarecer alguno de los delitos descritos en el artículo 282 bis 4[28], o cualquier delito de los previstos en el artículo 588 ter a[29]. Por último, solamente podrán participar en comunicaciones mantenidas en canales cerrados de comunicación, limitando así su competencia puesto que fuera quedarían "todos los contenidos informáticos de naturaleza abierta, como foros, blogs, chats o redes sociales con contenido público. Únicamente se podría usar para canales cerrados como mensajes privados de redes sociales o foros restringidos[30]".

A medida que el agente vaya tomando contacto con los sujetos a los que investiga, ira obteniendo información que pondrá en conocimiento del juez que autorizó la infiltración, siendo aportada posteriormente al eventual proceso en el que se juzguen los delitos objetos de investigación.

Para cerrar la regulación, se incluye la posibilidad de que el agente encubierto informático pueda intercambiar archivos ilícitos, siempre y cuando medie autorización judicial específica, así como analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.

---

[27] Referida, tal y como se encarga de aclarar el art. 282 bis 4, a la asociación de tres o más personas que llevan a cabo las conductas de forma permanente o reiterada.

[28] **a)** Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal. **b)** Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal. **c)** Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal. **d)** Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal. **e)** Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal. **f)** Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal. **g)** Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal. **h)** Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal. **i)** Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal. **j)** Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal. **k)** Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.
l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal. **m)** Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal. **n)** Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal. **o)** Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la LO 12/1995, de 12 de diciembre, de represión del contrabando.

[29] Reflejados en la nota a pie de página núm. 110.

[30] BUENO DE MATA, Federico. Comentarios críticos a la inclusión de la figura del agente encubierto virtual en la LO 13/2015. En: En: BUENO DE MATA, Federico. *Fodertics 4.0: (estudios sobre nuevas tecnologías y justicia)*. Granada: Comares, 2015. Págs.: 117-123. ISBN: 978-84-9045-274-5. Pág.: 121.

Este punto ha destapado otra de las críticas, y a su vez problemática, que rodean a esta nueva figura. Al no especificar qué se debe entender por "archivo ilícito", podemos llegar a pensar que el texto normativo está permitiendo al agente el uso de material pornográfico real que hayan podido obtener en otras investigaciones pasadas. Ante esta idea, lo más lógico es pensar en material pornográfico simulado, o pseudopornografía artificial y virtual, de manera que bajo ninguna circunstancia entre los archivos intercambiados estén presenten menores de edad reales sino simulados mediante cualquier artificio que resulte útil. Veremos con el paso del tiempo, cuáles son los pronunciamientos de nuestros tribunales en torno a este aspecto.

Así mismo, también se ha planteado la posibilidad de que una vez abierto el proceso, la parte sobre la que se construye la acusación plantee la nulidad del proceso alegando haber sido el delincuente inducido al delito por parte del agente encubierto. En este caso estaríamos ante un delito provocado, existente "cuando los agentes implicados -ya sean miembros de las fuerzas de seguridad o personas que actúen según sus instrucciones- no se limitan a investigar actividades delictivas de una manera pasiva, sino que ejercen una influencia tal sobre el sujeto que le incitan a cometer un delito que, sin esa influencia, no hubiera cometido, con el objeto de averiguar el delito, esto es, aportar pruebas y poder iniciar un proceso"[31].

Por lo tanto, y para que no queden dudas en torno a esta novedosa figura, podemos definir al agente encubierto en Internet "como un empleado o funcionario público que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la Red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la red" mediante "la ocultación de la verdadera identidad policial, con el fin de establecer una relación de confianza que permita al agente integrarse durante un periodo de tiempo prolongado en el mundo en el que los "ciberdelincuentes" actúan, con la finalidad primordial, igualmente oculta, de obtener la información necesaria para desenmascarar a los supuestos criminales"[32].

[31] **STEDH 1 marzo 2001 (TEDH 2011/26),** párrafo 42.
[32] BUENO DE MATA, Federico. El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia. En: PÉREZ-CRUZ MARTÍN, Agustín-J. FERRREIRO BAAMONDE, Xulio. NEIRA PENA, Ana María. *Los retos del Poder Judicial ante la sociedad globalizada.* A Coruña: Universidade da Coruña, 2012. Págs.: 295-306. ISBN**:** 978-84-9749-501-1. Pág.: 297.

III. ESTUDIO JURISPRUDENCIAL A TENOR DEL PUNTO ANTERIOR PREVIO A LA REFORMA DE LA LEY DE ENJUICIAMIENTO CRIMINAL

Antes de que tuviera lugar la reforma acaecida por vía de la LO 13/2015, en el ámbito de las investigaciones desarrolladas en nuestro país tenían lugar la práctica de las diligencias expuestas anteriormente a pesar de no estar provistas de regulación. En esta situación de incertidumbre, fueron nuestros Tribunales los que, una vez más, se encargaron de llenar esta laguna jurídica fijando el régimen en torno al cual, cada una de ellas debían ser practicadas.

1. La interceptación de las comunicaciones telefónicas y telemáticas (Art. 588 ter a. – Art. 588 ter m.)

Siguiendo el orden anteriormente expuesto, la interceptación de las comunicaciones telefónicas y telemáticas es posiblemente la diligencia sobre la que más pronunciamientos encontramos.

Desde la década de los 90, se puede observar cómo tanto el Tribunal Constitucional como el Tribunal Supremo, comenzaban a sentar y de una manera amplia, las bases de esta injerencia. Centrándose en la necesidad de una resolución judicial suficientemente motivada, el Tco. dictó varias sentencias siguiendo el mismo razonamiento: "el derecho al secreto de las comunicaciones sólo puede ser limitado mediante una resolución judicial suficientemente motivada. La existencia de un mandamiento judicial autorizando la intervención, junto con la estricta observancia del principio de proporcionalidad en la ejecución de esta diligencia de investigación, constituyen exigencias constitucionalmente inexcusables que afectan al núcleo esencial del derecho al secreto de las comunicaciones"[33]. Por lo tanto, no es suficiente con una resolución judicial habilitante genérica y lacónica, debiendo motivarse en cada caso la necesidad de la diligencia "ya que la motivación es la única vía de comprobación de que se ha llevado a cabo la ponderación judicial que constituye la esencial garantía de la excepción a la inviolabilidad de las comunicaciones" [34].

De una manera más concisa, el **TS en su sentencia núm. 288/1998**[35] agrupa en su FJ Tercero 10 requisitos para que las intervenciones telefónicas se consideren válidas: "1) la exclusividad jurisdiccional de tales intervenciones; 2) la excepcionalidad de la medida; 3) su proporcionalidad[36]; 4) la limitación temporal; 5) la especialidad del hecho delictivo;

[33] Localizable en el FJ Tercero de la **STco. 6 junio 1995 (RTC 1995/86),** y posteriormente en la **STco. 26 marzo 1996 (RTC 1996/49)** también el FJ Tercero.
[34] **STco. 26 marzo 1996 (RTC 1996/54),** FJ Séptimo.
[35] **STS 26 febrero 1998 (RTC 1998/1467).**
[36] Antes de la reforma de la LECrim, la proporcionalidad de la medida también se ponía en relación con el tipo de delito que se estuviera investigando, tal y como sucede en la actualidad con la introducción del

6) el que la medida deberá recaer únicamente sobre los teléfonos de las personas indiciariamente implicadas, sean los titulares o usuarios habituales de los mismos; 7) la existencia de un procedimiento, previo o simultáneo a la autorización de la medida; 8) la existencia previa de indicios[37] de comisión de algún delito (si bien, como quiera que la medida no es posterior a su descubrimiento, sino que se dirige a su averiguación, bastará para acordarla la existencia de indicios o sospechas racionales del delito que se investigue y que, por ello, sólo está en fase de presunción); 9) el riguroso control judicial de la medida, tanto en su ordenación como en su desarrollo y cese; y 10) la suficiente motivación de la correspondiente resolución judicial"[38]. Estos requisitos se encuentran desarrollados por una resolución posterior[39], encargada a su vez de incluir uno nuevo: "la finalidad exclusivamente probatoria de las interceptaciones para establecer la existencia de delito y descubrimiento de las personas responsables del mismo"; manteniéndose a lo largo de los años por la doctrina de manera inalterable[40].

A pesar de que han transcurrido en torno a 20 años desde que estas resoluciones vieron la luz, en ellas se recogen aspectos idénticos a los que ahora se han plasmado en la nueva LECrim mediante los artículos 588 bis a., 588 ter a., 588 ter b., 588 ter f., 599 ter g.

No obstante, éstas no son las únicas similitudes que se dan con la regulación actual. La **STS 18 junio 2008 (RJ 2008/3664),** ya amparaba en su FJ Segundo la facultad de las partes para poder acceder a las grabaciones y transcripciones realizadas: "Tales requisitos, son los propios que permiten la valoración directa por el Tribunal sentenciador de todo el caudal probatorio, y que por ello se refieren al protocolo de incorporación al proceso, siendo tales requisitos la aportación de las cintas originales íntegras al proceso y la efectiva

---

artículo 588 ter a. Así lo demuestra la **STco. 3 abril 2006 (RTC 2006/104),** al considerar que una intervención telefónica respeta el principio de proporcionalidad, "cuando su finalidad es la investigación de una «infracción punible grave, en atención al bien jurídico protegido y a la relevancia social del mismo»". Por lo tanto la calificación de la penal legítimamente prevista influía en la procedencia de la injerencia.

[37] Sobre los indicios es reseñable la **STS 28 septiembre 2009 (RTC 2009/197)**, la cual nos especifica qué debemos entender por los mismos en su FJ Cuarto: "Indicios que son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento. «La relación entre la persona investigada y el delito se manifiesta en las sospechas que, como tiene declarado este Tribunal, no son tan sólo circunstancias meramente anímicas, sino que precisan para que puedan entenderse fundadas hallarse apoyadas en datos objetivos, que han de serlo en un doble sentido. En primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control y en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito, sin que puedan consistir en valoraciones acerca de la persona". Esta doctrina ha sido reproducida en sentencias posteriores como la **STS 7 abril 2011 (RJ 2011/3341)**, o la **STS 18 abril 2013 (RJ 2013/8007)**.

[38] En palabras del Tribunal Constitucional, dicha autorización judicial habilitante debe contener "datos relativos al marco espacial –líneas telefónicas delimitadas–, temporal –plazos–, objetivo –hechos delictivos investigados– y subjetivo –personas conectadas con los hechos delictivos y titulares o usuarios de las líneas telefónicas– de la misma". Así se refleja en la **STco. 3 abril 2006 (RTC 2006/104),** FJ Segundo.

[39] **STS 7 marzo 2003 (RJ 2003/2815)**, FJ Primero

[40] Ejemplo de ello es la **STS 6 julio 2012 (RJ 2012/9445)**, sobre el desmantelamiento de una red que introducía alijos de hachís en las costas de Cádiz en la que se reproducen los 11 requisitos de una manera exacta en su FJ Octavo.

disponibilidad de este material para las partes junto con la audición o lectura de las mismas en el juicio oral lo que le dota de los principios de oralidad o contradicción"[41].

La jurisprudencia también ha recogido desde hace años la posibilidad de prorrogar la medida una vez acordada, precisando cual serían los requisitos en estos supuestos. En este punto podemos destacar la **STS 10 mayo 2011 (RJ 2011/5731),** por ser la encargada de recoger y unificar numerosas sentencias en las que se trata este tema, pudiendo destacar los siguientes puntos:

- Las exigencias de motivación sobre las resoluciones judiciales que habilitan la medida deben ser igualmente observadas en las prórrogas. Para ello el Juez "debe conocer los resultados de la intervención con carácter previo a acordar su prórroga y explicitar las razones que legitiman la continuidad de la restricción del derecho, aunque sea para poner de relieve que persisten las razones anteriores, sin que sea suficiente una remisión tacita o presunta a la inicialmente obtenida" (FJ Segundo).
- Respecto a la información que debe ser trasladad al Juez para que evalúe la procedencia de la prórroga, "sería suficiente con las transcripciones parciales de las conversaciones grabadas, sin acompañamiento de las cintas[42]" (FJ Segundo).
- Se considera cumplido el control judicial durante la prorroga cuando "los Autos de autorización y prórroga fijen periodos para que la fuerza actuante dé cuenta al Juzgado del resultado de las intervenciones, y que el órgano judicial efectúe un seguimiento de las mismas y conozca los resultados de la investigación" (FJ Segundo).

Nuestros Tribunales también se han pronunciado sobre las polémicas obtenciones por parte de la policía de numeraciones IMSI, IMEI y direcciones IPs. Comenzando con las numeraciones IMSI e IMEI, a pesar de que la mayoría de la doctrina considera que su obtención no precisa de autorización judicial por encontrarse fuera de la cobertura del artículo 18.3 de la CE[43], existen resoluciones con una postura contraria[44]. En mi opinión es

[41] Posteriormente plasmado de una manera idéntica en el FJ Cuarto de la **STS 6 julio 2009 (RJ 2009/5977)**. Sentencia muy completa y recomendable su lectura al desarrollar a lo largo de su FJ Cuarto las consecuencias que se derivan de la judicialidad, excepcionalidad y proporcionalidad de la medida. Así mismo pone de manifiesto la doble naturaleza que poseen este tipo de intervenciones "ya que pueden operar en el proceso como fuente de prueba y por tanto como medio de investigación, o pueden operar como prueba directa en sí".

[42] El Tribunal Constitucional se ha pronunciado en el mismo sentido, pudiendo citar como ejemplo la **STco. 27 abril 2010 (RTC 2010/26),** debiendo acudir a su FJ Cuarto: "para dicho control no es necesario que la policía remita las transcripciones íntegras y las cintas originales y que el Juez proceda a la audición de las mismas antes de acordar prórrogas o nuevas intervenciones, sino que resulta suficiente el conocimiento de los resultados obtenidos a través de las trascripciones de las conversaciones más relevantes y de los informes policiales".

[43] Ejemplos de ello son la **STS 6 julio 2012 (RJ 2012/9445)**, **STS 23 enero 2007 (RJ 2007/2316)**, **STS 31 marzo 2010 (RJ 2010/5547), STS 19 mayo 2010 (RJ 2010/5821),STS 15 marzo 2011 (RJ 2011/2783)**, **STS 17 noviembre 2011 (RJ 2012/11372)**, o la **STS 20 mayo 2008 (RJ 2008/4387)** clarificadora de la postura jurisprudencial respecto a la captación del IMSI resumir de manera comprensible este asunto: "la recogida o captación técnica del IMSI no necesita autorización judicial, sin embargo, la obtención de su plena funcionalidad, mediante la cesión de los datos que obran en los ficheros de la operadora, sí impondrá el

la doctrina mayoritaria quien razona de una manera más proporcional puesto que no se puede equiparar la interceptación de una conversación o la obtención de un listado de llamadas, con un número con el cual ni se conoce el número concreto de teléfono móvil ni el usuario del mismo.

Sobre las direcciones IPs, podemos sacar a colación un caso donde la Policía Judicial de la Guardia Civil obtuvo un listado de IPs rastreando las redes de intercambio de archivos (Peer to Peer) para averiguar aquellos usuarios que descargasen o compartiesen archivos conteniendo fotografías o vídeos con contenido de pornografía infantil. En este supuesto, recogido en la **STS 9 mayo 2008 (RJ 2008/4648)**[45]**,** se considera que en el acceso a las direcciones IPS tampoco se precisa de autorización judicial puesto que es una información pública y ha sido el propio usuario quien ha introducido esa información en la red; "la huella de la entrada queda registrada siempre y ello lo sabe el usuario"[46].

A pesar de haber dado tanta importancia a la resolución judicial que autoriza la medida, existen en la práctica excepciones donde ésta no se reputa necesaria. Un supuesto curioso se recoge en la **STS 1 abril 2002 (RJ 2002/5444),** la cual considera que no existe vulneración del derecho al secreto de las comunicaciones en la interceptación por parte de la Guardia Civil, de un radiotransmisor a uno de los acusados, escuchando en consecuencia y de manera casual las conversaciones que desde el mismo se vertían[47].

2. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (Art. 588 quater a. – Art. 588 quater e.)

La primera tarea a realizar por nuestros Tribunales fue determinar si realmente los agentes podían llevar a cabo esta diligencia al no existir ningún tipo de regulación en la LECrim que abriese el camino, al contrario de lo sucedido con la interceptación de comunicaciones. Sobre este proceso resulta muy completo el análisis plasmado en la ya mencionada Circular 1/2013, de la Fiscalía General del Estado, en su punto 5.8.

Como base para responder esta cuestión se debe traer a colación la **STS 2 junio 2010 (RJ 2010/3489)**, dictada a raíz de cuestionar la validez de unas escuchas realizadas en los calabozos de las dependencias policiales a varios sujetos en calidad de detenidos. Dejando a un lado la doctrina sentada por el TEDH recogida en la resolución, nos

---

control jurisdiccional de su procedencia". Sin embargo, en caso de que sean las operadoras las que deben ceder el IMSI para poder obtenerlo, sí que se necesita autorización judicial.

[44] En la **STS 19 febrero 2007 (RJ 2007/1809),** el Tribunal Supremo considera que el derecho fundamental al secreto de las comunicaciones se extiende no solo al contenido de las conversaciones, sino también la captura del abonado o de usuario como la del código del termina, es decir, del IMSI (FJ Primero).

[45] El mismo razonamiento se localiza tanto en el FJ Cuarto de la **STS 12 noviembre 2008 (RJ 2009/167)**, como en el FJ Primero de la **SAP Madrid 23 octubre 2015 (ARP 2015/1261)**.

[46] FJ Primero.

[47] FJ Sexto: "la audición de las conversaciones que se mantenían a través de radioteléfonos que se encontraban indisposición de ser escuchadas por cualquier persona que se encontrara en las inmediaciones no supone lesión alguna al derecho que se invoca".

centraremos en el razonamiento llevado a cabo teniendo en cuenta nuestra propia normativa.

Tras incluir las comunicaciones que, de forma verbal y directa, puedan producirse entre dos o más personas en un lugar cerrado, sin mediación de artificio o aparato alguno dentro del ámbito de protección desplegado por el artículo 18.3 de la CE se cuestiona la posibilidad de que pueda alzarse el secreto de las comunicaciones, aún con resolución judicial habilitante, al haber existido controversias entre la propia doctrina pudiéndose diferenciar dos sectores claros: aquellos que "mantiene que la autorización judicial para la instalación de aparatos de escucha, transmisión y grabación en lugar cerrado está fuera del ámbito de aplicación del art. 579 de la LECrim" y los que "mantiene que la autorización judicial para la instalación de aparatos de escucha, transmisión y grabación en lugar cerrado está fuera del ámbito de aplicación del art. 579 de la LECrim[48]".

Para resolver este debate, en primer lugar, la Sala hace mención a la **STS 10 febrero 1998 (RJ 1998\948)[49],** haciendo suyo el razonamiento expuesto en la misma**.** Esta sentencia llega a concluir la legitimidad de la instalación de aparatos de escucha y grabaciones en una celda de prisión preventiva que fue acordada por el Juez Instructor basándose en dos ideas:

- No se puede diferenciar entre conversaciones telefónicas y cualquier otro tipo de conversación privada ya que al propio Tribunal Constitucional "no le resulta concebible que se proteja menos una conversación por ser telefónica -en cuanto pueda ser legítimamente intervenida por el Juez- y no lo pueda ser una conversación no telefónica de dos personas en un recinto cerrado"[50].
- Si la LOGP permite que las comunicaciones orales y escritas sean intervenidas motivadamente por el Director del establecimiento, dando cuenta a la autoridad judicial competente por vía del artículo 51.1, "mucho más cuando sea el propio Juez Instructor de la causa el que lo acuerde cuando su finalidad es precisamente garantizar una pluralidad de valores en una sociedad democrática que no pueden desconocerse"[51].

En segundo lugar, centrándose en la regulación otorgada por la LOGP, y partiendo de la idea expuesta en el párrafo inmediatamente superior, considera que no ha existido vulneración del derecho al secreto con la colocación de medios ocultos de grabación audiovisuales (captación de imagen y sonido) en las celdas de los calabozos, habiendo sido acordado por el Juzgado de Instrucción apoyándose en el artículo 579.2 LECrim, del cual destaca su proporcionalidad y cautela al haber prohibido la instalación de los aparatos de

[48] FJ Tercero.
[49] Recoge un supuesto muy similar, al plantearse si la autorización judicial para la instalación de aparatos de escucha y grabaciones, mediante aparatos en lugar cerrado, en concreto en una celda de prisión preventiva cumple la exigencia de previsión y reserva legal que legitima tal injerencia en el ámbito del derecho fundamental a la intimidad personal y al secreto de las comunicaciones.
[50] FJ Tercero.
[51] FJ Tercero.

escucha "en el lugar donde aquéllos tengan acceso a la entrevista reservada con su letrado dado que el imputado puede revelar a su letrado los secretos que quedan bajo la reserva del secreto profesional"[52].

A pesar de la amplia doctrina que acoge este razonamiento, no todas las resoluciones se han dictado en este sentido. Ejemplo de ello es la **STCco. 22 septiembre 2014 (RTC 2014/145)[53]**, al considerar nula la intervención de comunicaciones verbales en dependencias policiales por entender carente de cobertura legal la resolución judicial que lo autorizaba.

En cuanto a las exigencias para poder llevar a cabo la intervención, la Audiencia Provincial de Lleida en una resolución relativamente reciente[54], señala al mandamiento judicial como el instrumento habilitante para la intromisión y recuerda la proporcionalidad[55] que debe existir en la medida, tal y como hace la doctrina de manera reiterada.

Sin embargo, las grabaciones como prueba en un proceso no sólo pueden introducirse en el mismo a través de una diligencia llevada a cabo por la Policía Judicial. También es posible que las propias partes sean quienes, habiendo grabado ellas mismas una conversación, las lleven ante el juez del caso. En estos casos se deben tener en cuenta los siguientes aspectos:

1. Al tratarse de una grabación privada obtenida por el interlocutor, no es obviamente exigible una autorización judicial motivada que sólo se requiere para la interceptación de conversaciones de terceros[56].
2. Si es uno de los protagonistas de la conversación quien decide grabarla, la aportación de las mismas al proceso "la jurisprudencia ha señalado que la grabación que un particular haga de sus propias conversaciones, telefónicas o de otra índole, no suponen el atentado al secreto de las comunicaciones (STS 20-2-2006 (RJ 2006, 2151) ; STS 28-10-2009 (RJ 2009, 7809) , nº 1051/2009)"[57].

---

[52] FJ Quinto.

[53] También se puede citar la **SAN 13 abril 2015 (JUR 2015/135793)**, acogiendo la misma deducción que el Tribunal Constitucional.

[54] **SAP Lleida (Sección 1ª) 19 junio 2014 (ARP 2014\1006).**

[55] "Proporcionalidad entre el sacrificio del derecho fundamental al que afecta la diligencia acordada y los logros que se esperan obtener con la misma en el proceso penal; proporcionalidad que debe ser ponderada tanto en relación con la gravedad penal de los hechos objeto del proceso como en relación con la probable efectividad de la medida y su difícil sustitución por otras menos restrictivas, lo que supone que haya de valorarse tanto la entidad del delito o delitos que se van a investigar, como la intensidad de los indicios acerca de su comisión, aunque en modo alguno puede exigirse la certeza en la comisión del delito o en la intervención de personas concretas" (FJ Primero).

[56] Así se reproduce literalmente en el FJ Segundo de la **STSJ Andalucía 12 junio 2013, Granada (ARP 2013/707).**

[57] **STS 24 junio 2011 (RJ 2011/5133),** FJ Sexto. Esta excepción a la resolución judicial habilitante, se ha mantenido tras la reforma de la LECrim, tal y como se puede apreciar en la **STS 15 julio 2016 (RJ 2016/3758)**: "la aportación al proceso de grabaciones de conversaciones particulares realizadas por uno de sus protagonistas no vulnera el derecho al secreto de las comunicaciones, pues este derecho no puede esgrimirse frente a los propios intervinientes en la conversación" (FJ Séptimo).

3. En cuanto al derecho a la intimidad, se plantea la duda de si éste podría verse afectado en este tipo de actuaciones. A pesar de existir resoluciones en las que se afirma que "una grabación subrepticia de una conversación entre cuatro personas realizada por una de ellas sin advertírselo a los demás, no ataca a la intimidad ni al derecho al secreto de las comunicaciones"[58], en mi opinión resultan más acertadas aquellas en las que se plantea una posible vulneración cuando "la conversación tuviera un contenido que afectara al núcleo esencial del derecho a la intimidad, ya sea en su ámbito personal o en el familiar"[59]. De esta manera, se instaura una especie de filtro, donde la vida personal y familiar de los interlocutores cobra relevancia.
4. En último lugar podrá considerarse ilegitima la grabación de una conversación privada cuando afecte al derecho constitucional a no declarar contra sí mismo y a no confesarse culpable. Esta transgresión podrá ser valorada por el Tribunal "cuando la persona grabada, de alguna manera, ha sido conducida al encuentro utilizando argucias con la premeditada pretensión de hacerle manifestar hechos que pudieran ser utilizados en su contra"[60]. Por ello, si se pretende la licitud de la prueba, es muy importante que la conversación grabada tenga lugar durante un encuentro en el que los interlocutores hayan decidido participar de manera libre, voluntaria, y espontánea.

Finalmente se debe aclarar qué sucede en caso de que tenga lugar por parte de los agentes un hallazgo casual una vez se ha habilitado la injerencia. Este supuesto se encuentra plasmado en la **STS 14 mayo 2013 (RJ 2013/3727)**, donde a raíz de unas escuchas de conversaciones que se llevaban a cabo dentro de un vehículo, previamente acordadas, se grabó una conversación relativa a un delito de torturas entre uno de los investigados y otra persona totalmente ajena al objeto de la investigación. Considera la Sala que en este caso no existe vulneración del derecho a la intimidad ni nulidad de tal conversación ya que ha derivado de una medida de injerencia válidamente adoptada y justificada, recordando que una intervención telefónica puede afectar los derechos de terceros ajenos a la investigación, sin que ello genere nulidades.

[58] **STS 1 marzo 1996 (RJ 1996/1886),** en su FJ Primero. Según la Sala de lo Penal del Tribunal, "las manifestaciones realizadas representaban la manifestación de voluntad de los intervinientes que fueron objeto de grabación de manera desleal desde el punto de vista ético pero que no traspasan las fronteras que el ordenamiento jurídico establece para proteger lo íntimo y secreto".

[59] Un ejemplo de fallo en el cual se tiene en cuenta el ámbito personal y familiar como factor para valorar una posible vulneración en el derecho a la intimidad es la **STS 16 mayo 2014 (RJ 2014/2937),** habiendo extraído el razonamiento de su FJ Tercero.

[60] Por este motivo el Tribunal Supremo considera inválida la grabación impugnada por la defensa en su sentencia citada en la nota de página inmediatamente anterior.

3. Utilización de dispositivos técnicos de captación de imagen, de seguimiento y de localización (Art. 588 quinquies a. – Art. 588 quinquies c.)

Comenzando con la captación de imágenes, la interpretación que a lo largo de los años nos han ofrecido nuestros Tribunales, concuerda con la actual regulación recogida en el artículo 588 quinquies a.

A raíz de la presentación de recursos en los que se alegaba principalmente la vulneración del derecho a la intimidad y la inviolabilidad domiciliaria, se fueron dictando diversas sentencias que han acabado sentando doctrina en torno a esta diligencia. Mediante el análisis de algunas de ellas, con el Tribunal Supremo como órgano enjuiciador, podemos destacar los siguientes puntos:

- Tomando como punto de partida el artículo 282 LECrim, consideran que no existe ningún obstáculo "para que las labores de investigación se extiendan a la captación de la imagen de las personas sospechosas de manera velada y subrepticia en los momentos en que se supone fundadamente que está cometiendo un hecho delictivo"[61]. Por lo tanto, se reputan válidos los sistemas mecánicos de captación de imágenes.
- Por lo que se refiere a la autorización, cuando la captación de imágenes se limite a lo que sucede en las vías o espacios públicos, ésta se encuentra autorizada por la Ley sin que precise de una resolución particular. Sin embargo, se necesitará autorización judicial expresa cuando la captación se realice en domicilios o lugares privados[62].
- En cuanto al aspecto más controvertido, la grabación de ventanas de un edificio desde un espacio público, la doctrina considera que "la autorización judicial siempre será necesaria cuando sea imprescindible vencer un obstáculo que haya sido predispuesto para salvaguardar la intimidad no siendo en cambio preciso el «Placet» judicial para ver lo que el titular de la vivienda no quiere ocultar a los demás"[63], es decir para ver lo que el titular de la vivienda no quiere ocultar a los demás.

La principal duda que se ha planteado en torno a los dispositivos técnicos de seguimiento y localización antes de que tuviera lugar la reforma de la LECrim, era si con ellos se estaba vulnerando el derecho a la intimidad de los sujetos que eran objeto de la misma, cuando no se poseía autorización judicial para su colocación. El Tribunal Superior

[61] **STS 14 octubre 2002 (RJ 2002\8963),** FJ Único.
[62] Así lo considera la **STS 15 febrero 1999 (RJ 1999/1918),** que a su vez recoge en su FJ Cuarto otras sentencias dictadas por esa misma Sala en el mismo sentido: "así se ha reconocido por esta Sala, en las SS. de 6-5-1993 [RJ 1993\3854], 7-2, 6-4 y 21-51994 [RJ 1994\702, RJ 1994\2889 y RJ 1994\3943], 18-12-1995 [RJ 1995\9196], 272-1996 [RJ 1996\1394], 5-5-1997 [RJ 1997\3628] y 968/1998 de 17-7 [RJ 1998\5843] entre otras)".
[63] **STS 13 marzo 2003 (RJ 2003/2662),** FJ Segundo.

de Justicia de Cataluña [64] para resolver esta cuestión se ha basado en doctrina reiterada del Tribunal Constitucional, según la cual, "si bien, de conformidad con el art. 18.3 CE , la intervención de las comunicaciones requiere siempre de autorización judicial, el art. 18.1 CE no prevé esa misma garantía respecto del derecho a la intimidad, de modo que se ha admitido la legitimidad constitucional de que en algunos casos y con la suficiente y precisa habilitación legal, la policía realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial"[65].

Además de la habilitación legal[66], al no exigirse previa autorización judicial, la medida debe cumplir otros requisitos que sirvan de "filtro" para proteger las garantías respecto al derecho a la intimidad. De la **STSJ Cataluña 23 julio 2015 (JUR 2015/241338)**[67] podemos extraer que, además en la colocación de dispositivos de localización y seguimiento, los agentes deben actuar atendiendo a un fin constitucionalmente legítimo y a las exigencias derivadas del principio de proporcionalidad.

Por lo tanto, siempre y cuando se cumplan las exigencias anteriormente impuestas, la colocación de dispositivos técnicos de localización y seguimiento se considerará una "diligencia de investigación legitima desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiera en su derecho fundamental que requeriría la intervención judicial"[68].

Sin embargo, en la colocación de estos dispositivos pueden concurrir circunstancias que determinen su nulidad como diligencia de investigación. Principalmente, podemos destacar tres:

- Que no se precise ninguna injerencia en ámbitos de la intimidad constitucionalmente protegidos, como la domiciliaria, para su colocación[69]. Esta injerencia tendría lugar, por ejemplo, con la entrada en los camarotes de una embarcación para poder instalar el dispositivo técnico del que se haga uso.
- Que con su instalación no deriven interrupciones electromagnéticas que puedan desviar el rumbo del objeto rastreado o poner en riesgo a sus ocupantes[70].
- Que la baliza instalada no sea empleada para "clase alguna de injerencia en las conversaciones o mensajes de los investigados"[71].

---

[64] **STSJ Cataluña 10 abril 2014 (ARP 2014/774)**
[65] Extraído de su FJ Tercero, punto 5.
[66] Otorgada en virtud del artículo 282 de la LECrim, al igual que sucede con la captación de imágenes.
[67] Se limita a reproducir de manera literal el razonamiento construido por la misma Sala en la sentencia del año anterior, para resolver un supuesto de vulneración del derecho a la intimidad por la colocación de balizas GPS en un vehículo de un sospechoso de la desaparición de dos personas.
[68] Así lo considera la **STS 5 noviembre 2013 (RJ 2013/7729)**, al estudiar la colocación por parte de miembros de Vigilacion Aduanera, de un dispositivo GPS en una embarcación.
[69] Así lo advierte en su FJ Segundo la **STS 22 junio 2007 (RJ 2007/5318)**.
[70] **SAN 26 julio 2008 (JUR 2008/246898)**, FJ Quinto.
[71] **STS 11 junio 2008 (RJ 2008/4655)**, FJ Séptimo.

4. Registro de dispositivos de almacenamiento masivo de información (Art. 588 sexies a. – Art. 588 sexies c.)

Con la regulación incluida por vía del artículo 588 sexies a., no se plantean dudas en torno a la necesidad de una autorización, no incluida en aquella resolución previa que habilita el registro domiciliario, en la que el juez de instrucción justifique cuáles han sido las razones que legitiman el acceso a los dispositivos. Este razonamiento judicial se puede localizar "en la misma resolución (habilitadora del registro domiciliario), ya en otra formalmente diferenciada"[72].

No obstante, al haber considerado la doctrina que "los documentos no integrados en un proceso de comunicación y almacenados en archivos informáticos bien en teléfonos móviles, ordenadores o asimilados, tendrían la consideración de simples documentos"[73], éstos únicamente resultan protegidos por el derecho a la intimidad[74]. Consecuentemente, en determinados casos muy tasados, se podrá acceder a los dispositivos de almacenamiento masivo de información sin que concurra resolución judicial habilitadora, en base al mismo razonamiento expuesto en el punto anterior [75].

Una de estas excepciones sí que se encuentra plasmada en la Ley a través del artículo 588 sexies c. 4., identificándose con los supuestos de urgencia en los que se aprecie un fin constitucionalmente legítimo[76]. Sin embargo, podemos destacar dos más:

- Cuando medie el consentimiento eficaz del sujeto particular que va a ser sometido a la diligencia, habiendo manifestado el Tco. "que éste no precisa ser expreso, admitiéndose también un consentimiento tácito […]reconociendo no sólo la eficacia del consentimiento prestado verbalmente, sino además la del derivado de la realización de actos concluyentes que expresen dicha voluntad"[77].
- Cuando es la persona afectada quien traslada directamente a la Policía el dispositivo del que es titular, donde se almacenan las pruebas del hecho ilícito y justificantes de la denuncia, sin que pueda apreciarse "vulneración de derecho alguno ya que se trata de una persona con acceso al ordenador, cotitular y por tanto de su uso"[78] ya que no es la policía quien lleva a cabo el descubrimiento, sino que su función es meramente certificadora.

---

[72] Éstas alternativas las recoge la **STS 17 abril 2013 (RJ 2013/3296)** en su FJ Octavo.

[73] Lo recuerda el FJ Segundo de la **STS 26 diciembre 2013 (RJ 2014/420)**, al hacer referencia a la STS 3 octubre 2007 (RJ 2007/6289).

[74] Salvo cuando se pretenda al acceso a correos electrónicos.

[75] En relación con la nota a pie de página 172.

[76] "El interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal" han sido considerados como causa legitima por la **STCo. 14 febrero 2005 (RTC 2005/25)**, FJ Sexto a.

[77] Sobre el consentimiento y la doctrina constitucional construida en torno a él, destaca la **STS 7 noviembre 2011 (RTC 2011/173).**

[78] Este supuesto excepcional puede apreciarse en la **STS 7 noviembre 2013 (RJ 2013/7468),** a raíz de la entrega a la Policía por parte de una madre de su ordenador, cuyo uso compartía con su pareja sentimental, al haber descubierto en él fotos de los pechos y genitales de su hija menor.

Manteniéndonos en el ámbito de la autorización judicial, podemos hablar de otra práctica peculiar que puede suceder en relación con el registro de dispositivos móviles, y que tampoco requeriría una resolución habilitante. Ésta tiene su origen en la distinción elaborada por la doctrina de la Sala de lo Penal del Tribunal Supremo, entre datos de comunicación y el acceso a datos de la agenda de contactos.

En el caso de los datos recogidos en una agenda de contactos del teléfono móvil[79], el derecho fundamental afectado en caso de que exista un acceso no autorizado por parte de los agentes al mismo, es el derecho a la intimidad personal y no el derecho al secreto de las comunicaciones[80], siempre y cuando no se acceda a funciones del teléfono móvil que pudieran desvelar procesos comunicativos como sucedería en caso de acceso al registro de llamadas entrantes y salientes.

Como ya he repetido en apartados anteriores, el derecho a la intimidad no es absoluto, por lo que puede ceder en determinadas circunstancias siempre y cuando concurra un fin constitucionalmente legítimo, habilitación legal[81] y se respete el principio de proporcionalidad de la medida.

Por lo tanto, los agentes podrán acceder a las agendas de contactos presentes en los teléfonos móviles sin necesidad de autorización judicial motivada, en aquellos "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"[82].

5. Registros remotos sobre equipos informáticos (Art. 588 septies a. – Art. 588 septies c.)

En la jurisprudencia existente con anterioridad a la reforma, únicamente podemos apreciar la comparación hecha entre esta diligencia y el registro de dispositivos de almacenamiento masivo de información, de manera que lo único que varía es el medio por el que se ejecuta, ya que en este tipo de registros no es necesaria una aprehensión física.

Por lo tanto, todas las exigencias y pautas establecidas por nuestros Tribunales para los registros de dispositivos de almacenamiento masivo de información han sido de aplicación analógica para la presente diligencia, y así se puede deducir de la lectura de la

[79] Son "equiparables a los recogidos en una agenda de teléfonos en soporte de papel": **STS 9 junio 2014 (RJ 2014\3398)**, FJ Octavo.
[80] Así se recoge en la **STco. 9 mayo 2013 (RTC 2013/115),** FJ Quinto.
[81] En el caso del acceso policial a las agendas de contactos recogidas en los teléfonos móviles, la **STS 25 abril 2010 (RJ 2010/4922),** considera como preceptos habilitadores para recoger los efectos, instrumentos y pruebas del delito y ponerlos a disposición judicial, y para practicar las diligencias necesarias para la averiguación del delito y el descubrimiento del delincuente los siguientes: a) Artículo 282 LECrim, b) Artículo 11.1 LO 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad, c) Artículo 14 de la LO 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana.
[82] **STco. 3 abril 2002 (RTC 2002/70),** FJ Décimo.

STco. 7 noviembre 2011 (RTC 2011/173) al concluir en su FJ Cuarto lo siguiente: "De lo expuesto, parece desprenderse que 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".

Consecuentemente, la resolución judicial previa que autorice la injerencia en el derecho fundamental a la intimidad cometida mediante el registro remoto es exigible todos los casos, salvo que medie consentimiento de la persona afectada o nos encontremos ante un supuesto de urgencia en el que concurra un fin constitucionalmente legítimo y el principio de proporcionalidad sea respetado.

6. El agente encubierto en Internet

A pesar de la introducción en la legislación de esta diligencia hace apenas un año, su práctica por parte de las Fuerzas y Cuerpos de Seguridad del Estado ya se llevaba a cabo con anterioridad. Un ejemplo de ello lo localizamos en la **STS 767/2007 3 octubre 2007 (RJ 2007/7297)**, pudiendo apreciar en sus antecedentes cómo el 25 de noviembre de 2005 el Fiscal de la Audiencia de Pontevedra, autorizó a un agente de la Guardia Civil para que actuara como agente encubierto en un ámbito internauta. Desde entonces, el agente mantuvo conversaciones a través de mensajería instantánea vía Messenger con el acusado y consiguió que le remitiera a su correo electrónico numerosos archivos informáticos conteniendo fotografías y vídeos, que obtenía visitando páginas webs de pornografía infantil, llegando a enviar 97 fotografías y 12 vídeos que reproducían la imagen pornográfica de un total de 115 menores de edad, muchos de ellos, menores de 13 años.

Lo mismo sucedió con la figura tradicional del agente encubierto en la década de los 90, al ponerse en práctica ésta medida antes de contar con la debida habilitación legal. Esta cuestión aparece solventada por la **STS 12 junio 2002 (RJ 2002/8419)**, en su FJ Segundo al considerar que a pesar de que en la fecha de los hechos no existía una previsión legal de las actuaciones del llamado agente encubierto, eso no significa que su actuación haya de considerarse ilícita ya que estamos ante "una actuación de la Policía Judicial en cumplimiento de las funciones que el ordenamiento le impone en relación a la averiguación de los delitos y al descubrimiento y aseguramiento de los delincuentes (artículo 126 de la Constitución), que será lícita si no se convierte en una provocación al delito y no afecta de otra forma a derechos fundamentales". Por lo tanto, a pesar de no contar con una regulación legal hasta finales del año 2015, las actuaciones de los agentes encubiertos llevadas a cabo a través de Internet no pueden considerarse fuera de Ley.

Desde que entrara en vigor la LO 3/2015, de 5 de octubre, nuestro sistema jurídico ya se ha pronunciado en relación con estas nuevas diligencias. Poniendo la atención en la

SJP Nº3 Gijón 6 julio 2016 (ARP 2016/843), además de recogerse en ella las razones[83] que motivan la autorización judicial en este tipo de medidas, la misma se encarga de pulir esta imposición al puntualizar "que las exigencias del derecho a la autodeterminación informativa, concernido de manera determinante, no son tan intensas en cuanto a la necesidad de intervención judicial". Por lo tanto, existen determinadas injerencias en este derecho que no requieren de "inexorablemente habilitación judicial".

A efectos prácticos conviene puntualizar cuáles son estas actuaciones relacionadas con figura del agente encubierto informático en las que no se va a requerir una resolución judicial habilitante. La **STS 6 noviembre 2013 (RJ 2013/7467)** nos da una primera idea al hablar de indagaciones policiales generadoras de una información de cierta calidad apta para dotar de fundamento la medida[84], ya que no se puede ser autorizada sin un "seguimiento previo, al objeto de contrastar los datos obtenidos y con el fin de evitar actuaciones precipitadas". Por lo tanto, lo que se está buscando antes de poner en marcha valiosos recursos de las diferentes FCSE, es una previa investigación en la que se corrobore la necesidad de la medida, y se construyan elementos de juicio que justifiquen la solicitud de la autorización judicial.

Así mismo, como ya poníamos de relieve en relación con las direcciones IPs, la **STS 14 julio 2010 (RJ 2010/3509)** se encarga de recordarnos que "no se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma"[85]. En consecuencia, todo lo que puedan recoger los agentes de la red para obtener información del caso antes de poner en marcha la diligencia es plenamente licito al no encontrarse amparados por el artículo 18.3 de la CE los datos que sean públicos.

Además, en todas estas actuaciones el agente no está obligado a exponer su verdadera identidad ya que "en las actuaciones dirigidas a la vigilancia, prevención y evitación de ilícitos en las redes informáticas cuya evidencia tiene lugar en fuentes abiertas en la web o canales no cerrados de comunicación, se viene sosteniendo que la ocultación de la condición de agente de la policía haciéndose pasar por un usuario más en la red, en principio no requiere autorización judicial"[86].

Una vez aclarado que la existencia de un contacto previo entre el recurrente y el agente encubierto, siempre y cuando encuentre su motivo en las labores de prevención y captación de información, en modo alguno conlleva una infracción de alcance constitucional[87], es interesante exponer qué régimen es aplicable al agente en este tipo de

[83] Principalmente son tres: las posibles injerencias en derechos fundamentales amparadas en un engaño o simulación; la afectación de un derecho de nueva generación como es la autodeterminación informativa, y la necesidad de dotar al agente encubierto de *inmunidad en sentido figurado* respecto de actuaciones que objetivamente podrían ser típicas y, por tanto, susceptibles de persecución penal.
[84] FJ Primero del Recurso del Carmelo.
[85] FJ Segundo.
[86] Extraído de la ya citada **SJP Nº3 Gijón 6 julio 2016 (ARP 2016/843).**
[87] En palabras del Tribunal Supremo, en su **STS 28 junio 2013 (RJ 2013/8067).**

actuaciones. La respuesta la podemos encontrar tanto en la **STS 6 febrero 2009 (RJ 2009/3065),** como en la **STS 29 diciembre 2010 (RJ 2011/135)** de manera repetida, siendo dos las principales consecuencias derivados de las tareas de investigación realizadas antes de llegar a tener el carácter de agente encubierto: la exención de responsabilidad criminal regulada en el apartado 5 del artículo 282 bis. no será aplicable a este periodo previo, pero en contraprestación, nada impide que pueda servir válidamente como testigo respecto a lo visto y oído en tiempo anterior.

IV. LA IMPORTANCIA DE LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA EN EL ORDEN JURISDICCIONAL PENAL

La sociedad en su conjunto es testigo a diario de la vertiente positiva de las nuevas tecnologías. Sin embargo, no podemos mirar hacia otro lado cuando a diario se pone de manifiesto la cara negativa de las mismas, al ser éstas protagonistas en nuevos tipos delictivos inexistentes hace unos años. Estas nuevas formas de transgresión de la Ley son conocidas como "ciberdelitos", "ciberdelincuencia", "crimen cibernético", etc. No obstante, me referiré a los mismos como delitos informáticos "por ser el término que se emplea con mayor frecuencia en la mayoría de los países de habla hispana"[88].

En la mayoría de las ocasiones, para que los delitos informáticos puedan llegar a ser enjuiciados, es necesario una prueba distinta a la que, hasta hace unos años, estábamos acostumbrados: la prueba electrónica. Y es en este punto donde las diligencias de investigación tecnológica cobran un papel fundamental al presentarse como la principal fuente de obtención de las mismas. Sin grabaciones captadas por videocámaras, conversaciones por vía telemática registradas en un ordenar interceptado por los agentes, un historial de páginas web obtenido mediante el registro remoto de un equipo informático, o las conversaciones de WhatsApp recogidas en un teléfono móvil, muchos de los ilícitos que más adelante desarrollaremos, quedarían exentos de castigo.

1. El fin de las diligencias: la consecución de la prueba electrónica

1.1. LA ACTIVIDAD PROBATORIA Y LA PRUEBA

En primer lugar, para poder comprender correctamente en qué consiste la prueba electrónica es importante ubicarla dentro de la estructura de cualquier proceso para entender así mismo su importancia. Tanto la prueba electrónica como cualquier tipo de prueba clásica o tradicional[89], se encuentran enmarcadas en la denominada fase probatoria del proceso.

Por lo tanto, es necesario, desde un punto de vista general aclarar qué entendemos por actividad probatoria, y, en consecuencia, por prueba.

Comenzando con la actividad probatoria por ser un concepto más claro y sobre el que no se generan demasiadas dudas, dentro del proceso ésta es la encaminada a "acreditar o convencer sobre la veracidad o certeza de un determinado hecho mediante percepciones

[88] VELASCO SAN MARTÍN, Cristos. *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet.* Valencia: Tirant lo Blanch, 2012. ISBN: 978-84-9004-981-5. Pág.: 50.

[89] Entendiendo como tales las enumeradas en el artículo 299.1 de la LEC: "Interrogatorio de las partes, documentos públicos, documentos privados, dictamen de peritos, reconocimiento judicial e interrogatorio de testigos".

sensitivas que nos proporcionan personas o cosas constituyendo fuentes, materias o instrumentos probatorios"[90] teniendo todas ellas como destinatario al juez o tribunal encargado del caso objeto de enjuiciamiento. Por lo tanto, probar es la actividad llevada a cabo por las partes en un proceso, encaminada a convencer al juez o tribunal de lo alegado en el mismo, siendo una fase esencial e indiscutible en todo proceso.

En esta labor llevada a cabo por las partes, las pruebas son un elemento esencial por ser el medio empleado para ello. En torno al concepto de prueba existe un amplio debate desde su aparición en el derecho a través las Siete Partidas[91], siendo muchos los autores que, desde entonces, se han pronunciado en torno a ella, pudiendo citar entre otros a BENTHAM, quien consideraba la prueba como "un hecho supuesto verdadero, que se considera que debe servir de motivo de credulidad sobre la existencia o no existencia de otro hecho. Así toda prueba comprende al menos dos hechos distintos: el uno que podemos llamar el hecho principal, el que se trata de probar que existe o que no existe, el otro el hecho probatorio, el que se emplea para probar el sí o el no del hecho principal"[92]; CARNELUTTI limita su ámbito de aplicación al estimar que "la prueba se usa como comprobación, de la verdad de una proposición; solo se habla de prueba a propósito de alguna cosa que ha sido afirmada y cuya exactitud se trata de probar; no pertenece a la prueba el procedimiento mediante el cual se descubre una verdad no afirmada"[93], siendo ésta la línea seguida por ARAZI al afirmar que "los hechos que son objetivo de prueba deben en el proceso civil, haber sido afirmados por las partes"[94].

Sin embargo, no es objeto del presente trabajo detenerse en esta controversia, sino optar por uno de los conceptos leídos hasta el momento para poder empezar con el análisis de la prueba electrónica. He escogido un concepto a mi juicio bastante específico y relacionado con la acepción dada de actividad probatoria, según el cual, prueba es "la vía por la que se alcanza el convencimiento psicológico de un juez o tribunal acerca de la hipotética verificación de las afirmaciones de las partes en el proceso"[95].

---

[90] BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0.* Valencia: Tirant lo Blanch, 2014. ISBN: 978-84-9053-483-0. Pág.: 93.

[91] Las Siete Partidas fue un cuerpo normativo redactado en Castilla por la época de Alfonso X, con la finalidad de intentar crear un código jurídico unificado en el Reino, algo que se puede observar con el título original que recibió la obra "*Libro de las leyes"* que posteriormente sería cambiado en el siglo XIV al de Siete Partidas. La obra en sí se puede considerar como uno de los legados más importantes de Castilla y contenía leyes que fueron usadas y ejecutadas en Iberoamérica hasta el siglo XIX tratando también temas filosóficos, morales y teleológicos. Sin lugar a dudas podemos hablar de un documento que entablo las bases de las leyes actuales. (http://historiageneral.com/2013/01/17/las-siete-partidas-leyes-de-la-antigua-castilla/) [Fecha de consulta: 28-08-2016].

[92] BENTHAM, M. Jeremías. *Tratado de las Pruebas Judiciales.* París: Bossange Frerres, 1825. Tomo Primero. Pág.: 19. (http://cdigital.dgb.uanl.mx/la/1080045433_C/1080045433_T1/1080045433_MA.PDF).

[93] CARNELUTTI, Francesco. *La prueba civil.* Buenos Aires: Arayú, 1982. ISBN: 950-14-0020-4. Pág.: 38.

[94] ARAZI, Roland. *La prueba en el proceso civil*. Buenos Aires: La Roca, 1998. ISBN: 950-9714-97-6. Pág.: 32.

[95] ILLÁN FERNÁNDEZ, José María. *La prueba electrónica, eficacia y valoración en el proceso civil.* Cizur Menor (Navarra): Aranzadi, 2009. ISBN: 978-84-9903-396-9. Pág.: 236.

1.1. LA PRUEBA ELECTRÓNICA: CONCEPTO

Como ya se ha avanzado en la introducción, el avance tecnológico unido a la presencia cada vez más reiterada de las TIC's[96] en prácticamente todos los ámbitos de la vida cotidiana de las personas, ha provocado de manera inevitable la aparición de nuevos "medios de prueba" conocidos ya popularmente mediante el término "prueba electrónica".

En la actualidad no contamos con ningún cuerpo normativo a nivel nacional ni internacional que nos ofrezca un concepto claro y único de lo que debemos entender por prueba electrónica. Por lo tanto, es necesario acudir a las aclaraciones prestadas por distintos autores para poder fijar una noción lo más aproximada posible.

Una de las opciones disponibles para poder comprender la prueba electrónica, es ponerla en relación con las pruebas clásicas o tradicionales ofreciendo así una definición general y en un sentido negativo, según la cual serían "aquellos que no aparecen relacionados en las antiguas leyes de enjuiciamiento (o, con mayor propiedad, aquellos que no pudieron estar en la mente del legislador al tiempo de promulgarse dichas leyes) y que son propiciados por los avances científicos o tecnológicos"[97]. Es decir, todos aquellos medios de prueba que no encajan dentro de los ya conocidos y regulados en el artículo 299.1 de la LEC, deben encuadrarse dentro de la prueba electrónica.

El hecho de que la prueba electrónica haya nacido de la evolución y aplicación de las nuevas tecnologías a la realidad que vivimos hoy en día, hace necesario un concepto mucho más específico y autónomo, separado de los medios probatorios conocidos hasta hace apenas unos años ya que se van a presentar cono instrumentos probatorios que requieren unos conocimientos especiales en su valoración, unos soportes distintos, etc.

En este sentido y siguiendo la línea de una concepción independiente, podemos considerar a la prueba electrónica como "aquella información obtenida a partir de un dispositivo electrónico o medio digital, el cual sirve para adquirir convencimiento de la certeza de un hecho"[98]; como "documentos electrónicos o a colecciones de datos procedentes de un sistema informático que pueden ser sometidos a los criterios de los peritos informáticos para determinar su autenticidad y ser aportados como prueba en juicio,

---

[96] Las Tecnologías de la Información y la Comunicación son un conjunto de servicios, redes, software y aparatos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario. (http://www.monografias.com/trabajos67/tics/tics.shtml#ixzz4IuE8WAzB) [Fecha de consulta: 28-08-2016].

[97] GÓMEZ DEL CASTILLO Y GÓMEZ, Manuel M. *Aproximación a los nuevos medios de prueba en el proceso civil.* (http://rabida.uhu.es/dspace/bitstream/handle/10272/1546/b1205663.pdf?sequence=1) [Fecha de consulta: 28-08-2016].

[98] INSA MÉRIDA, Fredesvinda, LÁZARO HERRERO, Carmen, GARCÍA GÓNZALEZ, Nuria. *Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad. Un proyecto europeo.* (http://www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1690-75152008000200009). [Fecha de consulta: 28-08-2016].

de manera que su contenido es relevante para el caso"[99]; o 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 *hardware,* y un elemento lógico o *software" [100],* siendo esta la acepción más completa de las vistas a mi juicio.

Finalmente, debemos destacar respecto de la prueba electrónica el carácter polifacético de la misma ya que al poder ser objeto de prueba y/o medio de prueba: "puede ser objeto de prueba, y así se habla de "probar un hecho electrónico", puede ser un medio de prueba y así se alude a "probar electrónicamente un hecho", o puede, simultáneamente, ser objeto y medio de prueba cuando se trata de "probar electrónicamente un hecho electrónico"[101].

1.2. LA PRUEBA ELECTRÓNICA, ¿MEDIO DE PRUEBA O FUENTE DE PRUEBA?

Como veremos en el título relativo a la regulación, el artículo 299 de la LEC en su apartado 2º[102] así como en el 3º[103], a la hora de regular los medios de prueba, incluye la posibilidad de aportar cualquier otro medio de prueba ante el tribunal, distintos de aquellos recogidos en los apartados anteriores del mencionado artículo, siempre y cuando pudiera obtenerse la certeza sobre hechos relevantes gracias a ellos. Así mismo incluye la posibilidad de aportar medios de reproducción de la palabra, sonido, etc., apartándose de la enumeración, hasta entonces cerrada, de los medios de prueba clásicos plasmados en el apartado 1º.

Por lo tanto, el legislador parece haber decidido "ampliar de forma ilimitada todos los medios de prueba que se puedan practicar. Es más, en la propia Exposición de Motivos de la Ley, XI párrafo V, se da a entender que una clasificación cerrada de los medios de

[99] Este concepto es popularizado por el Foro de las Evidencias Electrónicas, procediendo de la denominación inglesa "*electro evidence"*, habiendo sido extraído del artículo: Seminario de Evidencias Electrónicas en septiembre. http://www.foroevidenciaselectronicas.org/2011/07/28/seminario-de-evidencias-electronicas-en-septiembre/. [Fecha de consulta: 28-08-2016].

[100] BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0.* Valencia: Tirant lo Blanch, 2014. ISBN: 978-84-9053-483-0. Pág.: 103.

[101] ABEL LLUNCH, Xavier, PICÓ I JUNOY, Joan, et al. La prueba electrónica. Barcelona: Bosch, 2011. ISBN: 978-84-7698-955-5. Pág.: 26.

[102] "También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso".

[103] "Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias".

prueba no tiene sentido en los tiempos actuales, dados los avances y cambios tecnológicos que vivimos hoy en día"[104].

Esta aparente ampliación de los medios de prueba choca de lleno con la teoría presente hasta el momento, según la cual, "existen numerosas e ilimitadas fuentes de prueba", pero "por el contrario, los medios de prueba son limitados o al menos, conforme al art. 299, se contraen a constituir procedimientos mediante los cuales las fuentes de prueba se incorporan al proceso en condiciones útiles para servir de base adecuada a la resolución que le pone fin"[105].

Entonces, ¿realmente el legislador ha querido romper con el sistema *numerus clausus* característico de los medios de prueba, o, por el contrario, a la hora de redactar los apartados mencionados anteriormente se ha producido una confusión de términos? Como ya refleja BUENO DE MATA en su obra "*Prueba electrónica y proceso 2.0"* incluida en la bibliografía del presente trabajo, a la hora de responder la presente pregunta la doctrina está dividida: "por un lado CALVO SANCHEZ critica esta supuesta apertura probatoria al igual que ABEL LLUNCH […]. En el lado opuesto se sitúa otra parte de la doctrina como ORMAZÁBAL SÁNCHEZ o de la OLIVA"[106].

Como en muchos otros casos ha sido el poder judicial quien ha acabado con el debate al establecer lo siguiente: "Se regula pues, en la nueva L.E.C., la utilización de medios y soportes técnicos para la reproducción y archivo de imágenes, sonidos y datos de una manera autónoma, aun cuando no suponen propiamente nuevos "medios de prueba" independientes, sino nuevas fuentes de prueba"[107].

En conclusión, la prueba tecnología no está considerada como un nuevo medio de prueba en sí, sino como una de tantas fuentes de prueba, donde "la fuente de prueba electrónica, es el soporte (material) en el cual ha quedado grabado el hecho histórico que vamos a introducir en el proceso y el medio probatorio será la reproducción realizada ante el órgano jurisdiccional"[108]. Por lo tanto, toda prueba electrónica debe ser aportada al proceso a través de cualquiera de los medios de prueba enunciados en el artículo 299.1 de la LEC.

---

[104] DE LAS HERAS MUÑOS, Mar. Medios de prueba. Informática forense y peritaje informático. En: BUENO DE MATA, Federico. *Fodertics: estudios sobre derecho y nuevas tecnologías*. Santiago de Compostela: Andavira, D.L.2012. ISBN: 978-84-8408-692-5. Pág.: 222.

[105] ASENCIO MELLADO, José María. *La prueba documental. Concepto y regulación legal.* (http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbF1jTAAAUsDC1NDtbLUouLM_DxbIwNDY0MjQ0uQQGZapUt-ckhlQaptWmJOcSoA4ZERPTUAAAA=WKE) [Fecha de consulta: 30-08-2016].

[106] BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0.* Valencia: Tirant lo Blanch, 2014. ISBN: 978-84-9053-483-0. Pág.: 118 y 119.

[107] Así lo esclarece la **SAP Barcelona (Sección 13ª) 2 de mayo 2007 (JUR 2007/270189),** en su FJ Tercero.

[108] ILLÁN FERNÁNDEZ, José María. *La prueba electrónica, eficacia y valoración en el proceso civil.* Cizur Menor (Navarra): Aranzadi, 2009. ISBN: 978-84-9903-396-9. Pág.: 264.

1.3. NATURALEZA JURÍDICA DE LA PRUEBA ELECTRÓNICA

En este punto la discusión se centra en determinar si con la prueba electrónica nos encontramos ante una prueba documental o especial, o si por el contrario se trata de una prueba de reconocimiento judicial, requiriendo el examen directo por parte del órgano judicial. Es importante acláralo "pues de la decisión que se tome va a depender su régimen jurídico, y, especialmente en los aspectos en los que se detecten vacíos o lagunas legales, el régimen supletorio que, por analogía, haya de aplicarse"[109].

Para responder a esta cuestión se nos presentan tres teorías diferentes[110]: la teoría autónoma, la teoría analógica y la teoría de la equivalencia funcional.

La primera de ellas sostiene que la prueba electrónica "tiene una especificidad singular con respecto de los medios de prueba tradicionales, y en particular, de la prueba documental". La segunda de ellas, más acertada que la anterior, defiende que " los medios de prueba tradicionales y los nuevos medios de pruebas son de naturaleza equiparable y que en los nuevos medios de prueba el suporte electrónico o digital ha sustituido al soporte papel"; sin embargo, quedarían sometidos a distintas reglas de valoración de la prueba ya que el documento en soporte papel "queda sometido a las reglas de prueba tasada", y el documento en soporte electrónico "a las reglas de la sana critica", teniendo por lo tanto distinta eficacia probatoria. La última de las teorías, la más acertada a mi entender, equipara el documento en soporte papel al documento electrónico de manera que "toda declaración de voluntad asentada en un medio informático o electrónico tiene el mismo valor jurídico que los documentos cuyo soporte sea material, por tanto, los documentos en estudio producen efectos jurídicos y tienen la misma fuerza probatoria que los tradicionales"[111].

Es en la Exposición de Motivos[112] de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil donde encontramos la respuesta definitiva: "no es de excluir, sino que la ley lo prevé, la utilización de nuevos instrumentos probatorios, como soportes, hoy no convencionales, de datos, cifras y cuentas, a los que, en definitiva, haya de otorgárseles una consideración análoga a la de las pruebas documentales". Así mismo, el artículo 3.8[113] de la Ley 59/2003, de 19 de diciembre, de firma electrónica, también apoya esa equiparación con la prueba documental al igual que el artículo 24.2[114] de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

---

[109] URBANO CASTRILLO, Eduardo, MAGRO SERVET, Vicente. *La prueba tecnológica en la Ley de Enjuiciamiento Civil.* Cizur Menor (Navarra): Aranzadi, 2003. ISBN: 847671015. Pág.: 39 y 40.

[110] Extraídas de: ABEL LLUNCH, Xavier, PICÓ I JUNOY, Joan, et al. La prueba electrónica. Barcelona: Bosch, 2011. ISBN: 978-84-7698-955-5. Pág.: 107-113.

[111] ILLÁN FERNÁNDEZ, José María. *La prueba electrónica, eficacia y valoración en el proceso civil.* Cizur Menor (Navarra): Aranzadi, 2009. ISBN: 978-84-9903-396-9. Pág.: 254.

[112] En: XI, párrafo XIII.

[113] "El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio".

[114] "En todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental".

La jurisprudencia también apoya la analogía con la prueba documental, tal y como se refleja en la **STSJ de Madrid 6 de julio (AS 2004/2325)**[115]**,** al enunciar en su FJ primero lo siguiente: "el concepto de documento no puede interpretarse de una forma tan restrictiva que solo abarque representaciones escritas, muy al contrario, hay que considerar como tal todo objeto que cumpla la función de dar a conocer determinados elementos en el representados, bien por escrito, imágenes o sonidos".

Todo ello, junto con el dato esclarecedor de que "el 89,5% de los expertos jurídicos considera que la validez de la prueba electrónica, como un e-mail, la factura y la firma electrónica, es equivalente a la tradicional en los procesos judiciales"[116], parece posicionar la teoría de la equivalencia funcional como la más precisa.

1.4. REGULACIÓN DE LA PRUEBA ELECTRÓNICA

A pesar de los avances experimentados en la sociedad gracias a las TIC's, todavía no existe en nuestro país un cuerpo normativo encargado de regular la prueba electrónica, lo que da lugar a la existencia de una gran laguna jurídica entorno a la misma. Un método factible para luchar con este problema es poner la vista en la regulación dada a nivel tanto internacional como comunitario, antes de entrar en la que nos ocupa nivel estatal.

A. NORMATIVA INTERNACIONAL

La esfera internacional[117] ya se ha hecho eco de la necesaria adaptación de las leyes por parte de los países miembros, con la finalidad de eliminar el ciberespacio de la delincuencia, apostando por el intercambio de información del que disponen los estados, consiguiendo así una cooperación que tenga como resultado una correcta investigación penal. Esta reivindicación se ha encargado de llevarla a cabo la Asamblea General de la ONU mediante la adopción de las Resoluciones 55/63 y 56/121.

Así mismo existen varias Recomendaciones aprobadas por la Comisión de Naciones Unidas para el Derecho Mercantil Internacional "dirigidas a los gobiernos y a las organizaciones internacionales acerca del valor jurídico de los registros de ordenador".

Posteriormente tuvo lugar en Nueva York la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, cuya principal finalidad fue "facilitar la utilización de las comunicaciones electrónicas en el

[115] La cual, comparte el criterio expresado por la **STSJ Andalucía 28 de enero, Málaga (AS 2000/146).**

[116] REDACCIÓN NJ. *El 89,5% de los expertos jurídicos europeos equipara la validez de la prueba electrónica con la tradicional*. (http://noticias.juridicas.com/actualidad/noticias/26-el-89-5-de-los-expertos-juridicos-europeos-equipara-la-validez-de-la-prueba-electronica-con-la-tradicional/) [Fecha de consulta: 31-08-2016].

[117] Para la redacción de este punto se han realizado varias extracciones de: PÉREZ PALACÍ, José Enrique. *La prueba electrónica: Consideraciones*. (http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39084/1/PruebaElectronica2014.pdf) [Fecha de consulta: 31-08-2016].

comercio internacional garantizando que los contratos concertados electrónicamente y las comunicaciones intercambiadas por medios electrónicos tengan la misma validez y sean igualmente ejecutables que los contratos y las comunicaciones tradicionales sobre papel"[118].

Por lo tanto, aunque desde comienzos de siglo se ha puesto de relieve la insuficiencia normativa de la que somos víctimas la comunidad internacional en su conjunto, las normas que se han dictado desde entonces recogen una regulación escasa y puntual sin poder encontrar ninguna que englobe de manera completa y general unas pautas sobre las que cimentar la normativa nacional.

B. NORMATIVA COMUNITARIA

Relacionado con la prueba electrónica de una manera directa e indirecta, en la Unión Europea encontramos las siguientes referencias:

- Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, firmado por el Plenipotenciario de España, donde "encontramos ya el término "prueba electrónica" en su artículo 14.2.c) como forma de probar determinadas infracciones penales relacionadas con el mundo de las TIC's"[119].
- Decisión Marco 2008/978/JAI DEL CONSEJO, de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de pruebas. Posibilita en su Considerando 13, la búsqueda de datos electrónicos por parte de la autoridad de ejecución siempre y cuando éstos no se encuentren en el Estado de ejecución.
- Resolución AG-2008-RES-08[120]. Fue adoptada por la Asamblea General de la OIPC-INTERPOL, en su 77a reunión, celebrada en San Petersburgo (Rusia) del 7 al 10 de octubre de 2008, y por ella se aprueba el establecimiento de una Unidad de Análisis Informático Forense con la finalidad de, entre otras, "elaborar normas internacionales que regulen la búsqueda, el decomiso y la investigación de pruebas electrónicas", "dado el constante aumento del número de investigaciones internacionales relacionadas con pruebas electrónicas".
- Reglamento de la Unión Europea nº 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. Encargado de derogar la Directiva 1999/93/CE, con la finalidad de "reforzar y

---

[118] CNUDMI. *Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005).* (http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2005Convention.html) [Fecha de consulta: 31-08-2016].

[119] BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0.* Valencia: Tirant lo Blanch, 2014. ISBN: 978-84-9053-483-0. Pág.: 122.

[120] Texto íntegro en: https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwjY9MKD0fDOAhUJwxQKHQiLDg4QFggrMAI&url=http%3A%2F%2Fwww.interpol.int%2Fcontent%2Fdownload%2F5297%2F44458%2Fversion%2F4%2Ffile%2FAGN77RES08Es.pdf&usg=AFQjCNGfkFmI1EUI2JAPrd3DfMsfL6T8NQ. [Fecha de consulta: 31-08-2016].

ampliar el acervo que representa dicha Directiva[121]", la cual, "se refiere a las firmas electrónicas, sin ofrecer un marco global transfronterizo e intersectorial para garantizar unas transacciones electrónicas seguras, fiables y de fácil uso". Esta nueva regulación de la firma electrónica se plasma en los artículos 25 y ss.

- El Certificado Europeo sobre Cibercriminalidad y Prueba Electrónica: se trata de uno de los proyectos impulsados por el Cybex y se trata del "primer Certificado Europeo que proporciona formación técnica a jueces, fiscales y abogados sobre el Cibercrimen y el uso de la Prueba Electrónica"[122]. Así mismo "Este programa europeo conlleva también la creación del primer Fondo Documental Europeo sobre Cibercrimen y Prueba Electrónica al que los asociados tendrán acceso ilimitado, permitiendo de esta manera encontrar artículos y referencias de interés y actualidad relacionados con estos aspectos en toda Europa, además de jurisprudencia y legislación sobre la materia"[123].

C. NORMATIVA NACIONAL

Ya que por el momento no contamos en nuestro país con un cuerpo normativo destinado a regular la prueba electrónica, este apartado esta principalmente destinado a agrupar de la manera más sencilla y resumida posible, los distintos preceptos que nos acercan a una aceptación de la misma en nuestro sistema judicial.

El punto de partida lo encontramos, como no puede ser de otra manera en nuestra norma suprema: la Constitución Española. El artículo 24.2 de la CE[124] otorga a todos, el derecho a utilizar todos los medios de prueba pertinentes para poder defenderse sin establecer limitación ninguna[125] siempre y cuando sean pertinentes. Por lo tanto, mediante este artículo se "garantiza el principio de libertad de prueba, en virtud del cual las partes en

[121] Así se refleja en el Considerando 3 del propio Reglamento.

[122] INSA MÉRIDA, Fredesvinda. *El Certificado Europeo sobre Cibercriminalidad y Prueba Electrónica (ECCE): Un gran proyecto de formación para los profesionales del mundo jurídico.* (http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbF1jTAAAUMzSwNLtbLUouLM_DxbIwMDSwMjIzOQQGZapUt-ckhlQaptWmJOcSoA-tOpMTUAAAA=WKE). [Fecha de consulta: 31-08-2016].

[123] MADARIAGA, Bárbara. *Llega la primera Certificación Europea sobre Cibercriminalidad y Pruebas Electrónicas.* (http://www.dealerworld.es/seguridad/llega-la-primera-certificacion-europea-sobre-cibercriminalidad-y-pruebas-electronicas). [Fecha de consulta: 31-08-2016].

[124] "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".

[125] Aclarando no obstante la doctrina constitucional en innumerables sentencias, que éste "no comprende un hipotético derecho a una actividad probatoria ilimitada, atendiendo a la naturaleza del derecho como de configuración legal, por lo que su ejercicio habrá de acomodarse a las exigencias del proceso y a las normas legales que lo prevean, cuya interpretación en relación a la admisión de los medios de prueba corresponde a los Tribunales ordinarios en ejercicio de sus funciones jurisdiccionales" tal y como se desprende de la **STco. 17 septiembre 1999 (RTC 1999/219).**

un proceso tienen derecho a la admisión y practica de cualquier prueba, esté o no prevista por la ley, con los límites de pertinencia, licitud y utilidad"[126].

Partiendo de esta base, la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil desde su texto original publicado el 8 de enero de 2000 trata de proporcionar una adecuada cobertura legal a los diversos medios probatorios que iban surgiendo distintos de los conocidos como "tradicionales o clásicos", abriéndose así a la realidad social. Siguiendo el orden reflejado en la Ley, estos son los artículos encargados de trazar el marco legal:

- Artículo 299, apartado 2: enumera de manera "cerrada" dos tipos de medios de prueba que junto con los del apartado 1, también podrán ser admitidos:
    - Medios de reproducción de la palabra, el sonido y la imagen: por ejemplo, una grabación de sonido que se encuentre recogida en un lector MP3 o un fax.
    - Instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas: como un ordenador, con la información obtenida en su disco duro, un DVD o un correo electrónico.

- Artículo 299, apartado 3[127]: al contrario que su antedicho, éste no contiene una relación cerrada, sino que "en este último caso la ley reconoce la posibilidad de existencia de fuentes de prueba no predeterminadas, quedando al arbitrio judicial la forma de articulación del medio de prueba"[128]. Por consiguiente, deja la puerta abierta a la posible aparición de nuevas fuentes de prueba que puedan manifestarse en el futuro, desconocidas hasta el momento.

- Artículos 382 al 384: encargados de regular el modo a seguir por las partes para introducir las anteriores fuentes de prueba en el proceso, la ley hace una diferenciación en función de que estemos ante instrumentos de filmación, grabación o semejantes (arts. 382 y 383) o ante instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso (articulo 384). En el primero de los casos, ésta prueba se deberá acompañar de una transcripción escrita[129] de aquellas palabras que se obtengan de los mismos, y en el segundo de los casos los instrumentos mencionados "serán examinados por el tribunal por los medios que la parte proponente aporte o que el tribunal disponga utilizar"[130]. A pesar de esta diferenciación, no todos los autores se encuentran de acuerdo con ella al considerar

[126] ILLÁN FERNÁNDEZ, José María. *La prueba electrónica, eficacia y valoración en el proceso civil.* Cizur Menor (Navarra): Aranzadi, 2009. ISBN: 978-84-9903-396-9. Pág.: 330.
[127] "Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias".
[128] JUANES FRAGA, Enrique. Artículo 90. En: DE LA VILLA GIL, Luis Enrique. *Ley de procedimiento laboral: comentada y con jurisprudencia.* Las Rozas (Madrid): LA LEY, 2006. ISBN: 978-84-9725-690-2. Pág.: 706.
[129] A diferencia del texto original de la LEC donde se fijaba como una opción, no como un deber: "la parte podrá acompañar en su caso, transcripción escrita de las palabras…".
[130] Apartado 1 del artículo 384 de la LEC.

"que semejante distinción carece de regulación alguna y de contenido que justifique su tratamiento diferenciado, por lo que se debe integrar unitariamente las normas de ambas fuentes de prueba para cubrir las respectivas lagunas"[131], o como comúnmente se diría, la unión hace la fuerza.

- Artículo 318: destaca por conceder a los documentos públicos la misma fuerza probatoria independientemente de que sean presentados en soporte papel o mediante documentos electrónicos, otorgando a ambos medios la misma consideración.

  Por lo tanto, es en el orden jurisdiccional civil donde se localiza la regulación más completa a través de la LEC, por lo que es necesario llevar a cabo una aplicación analógica de la misma al resto de órdenes jurisdiccionales. Ésta es posible por vía del artículo 4 de la misma, encargado de establecer el carácter supletorio de la Ley de Enjuiciamiento Civil al exponer lo siguiente: "En defecto de disposiciones en las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, serán de aplicación, a todos ellos, los preceptos de la presente Ley".

Finalmente, existen muchas otras normas que regulan múltiples conceptos o métodos relacionados de una manera u otra con la prueba electrónica, mencionando a modo ejemplificativo:

- Artículo 26 del Código Penal: es el soporte del documento donde ponemos le punto de mira ya que según éste artículo "ya no es necesario que sea papel sino que puede consistir en cualquier sustancia o medio material capaz de recoger una información (…): soportes ópticos como el CD-ROM o el DVD, fotografías, disquetes, cintas de vídeo, grabaciones magnetofónicas, tarjetas electromagnéticas"[132].

- Artículo 230 de la Ley Orgánica del Poder Judicial: lo más llamativo en relación con la prueba electrónica es que obliga tanto a Jugados, Tribunales y Fiscalías a utilizar medios técnicos, electrónicos, informáticos y telemáticos, para el desarrollo de su actividad, y por lo tanto, también para poder analizar las fuentes de prueba electrónicas aportadas por las partes que requieran de los mismos (ej.: la cibernavegación llevada a cabo por un juez para examinar una página web que ha sido introducida como fuente de prueba en un proceso judicial).

- A diferencia del tema objeto de estudio, el documento electrónico cuenta regulación más completa a lo largo del Título VI del RD 1671/2009, de 6 de noviembre.

[131] ABEL LLUNCH, Xavier, PICÓ I JUNOY, Joan, et al. La prueba electrónica. Barcelona: Bosch, 2011. ISBN: 978-84-7698-955-5. Pág.: 103.

[132] RUIZ SERRA, Joana. *Artículo 26 del código penal: el documento (España)* (http://www.monografias.com/trabajos104/articulo-26-del-codigo-penal-documento/articulo-26-del-codigo-penal-documento.shtml#ixzz4KG2zNNuB) [Fecha de consulta: 14-09-2016].

1.5. TIPOLOGÍA

Para determinar la clase de pruebas electrónicas que existen, una opción sería hacer referencia a los tipos específicos que conocemos hasta el momento como pude ser el fax, sistemas de mensajería instantánea, la información extraída de un disco duro, etc. Sin embargo, el constante avance tecnológico pude dar lugar a la aparición de muchos otros hasta ahora inexistentes, por lo que lo más conveniente es "clasificar las distintas pruebas electrónicas dentro de un sistema de *numerus apertus* basado en categorías de pruebas electrónicas y no en figuras concretas"[133]. Esta opción doctrinal es la adoptada por autores como BUENO DE MATA, DE URBANO CASTRILLO o BUJOSA VADELL.

De esta manera encontraríamos "dos grandes grupos en los que se aplican las tecnologías digitales, aunque de distinta manera"[134]:

- **Medios de prueba relativamente nuevos**

  En este grupo a su vez encontraríamos otros tres subgrupos[135]:

  - Aquellas creadas directamente a través de la informática: como por ejemplo un correo electrónico.
  - Las procedentes de medios de reproducción o archivo electrónico: las fotografías extraídas de un teléfono móvil, o un vídeo encontrado en una cámara fotográfica.
  - Las que se presentan mediante instrumentos informáticos: un pen-drive, bases de datos, etc.

- **Medios de prueba en los que se observa una mayor cercanía a los medios de prueba tradicionales**

  En este grupo se englobarían aquellas pruebas tradicionales que se encuentran puestas en relación de alguna manera con las nuevas tecnologías ya sea por el empleo de las mismas para poder llevarse a cabo, o como medio para facilitar su práctica rompiendo barreras como puede ser la declaración de un testigo a través de la videoconferencia.

---

[133] BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0.* Valencia: Tirant lo Blanch, 2014. ISBN: 978-84-9053-483-0. Pág.: 131.

[134] BUJOSA VADELL, Lorenzo M. La valoración de la prueba electrónica. En: BUENO DE MATA, Federico. *Fodertics 3.0: (estudios sobre nuevas tecnologías y justicia)*. Granada: Comares, 2015. ISBN: 978-84-9045-239-4. Pág.:77.

[135] URBANO CASTRILLO, Eduardo. *La valoración de la prueba electrónica.* Valencia: Tirant lo Blanch, 2009. ISBN: 978-84-9876-445-1. Pág.:52.

2. La aplicación de las diligencias: los delitos informáticos más destacados

Para comenzar, debemos fijar una definición lo más sencilla posible de delitos informáticos, comprensible por cualquier persona con unos conocimientos mínimos en informática, considerándolos, por lo tanto, como "toda acción típica, antijurídica y culpable cometida contra o por medio de la utilización de procesamiento automático de datos o su transmisión"[136].

Esta descripción dada no solo nos permite una fácil comprensión, sino que a su vez pone de manifiesto la doble cara de los sistemas informáticos no sólo como objeto de ataque, sino también como medio para llevar a cabo el mismo. De esta manera podemos diferenciar dos tipos de ilícitos: los delitos computacionales y los delitos informáticos "sensu stricto". Los primeros se identifican con aquellos delitos tradicionales en los que los delincuentes comienzan a utilizar como un medio especifico de comisión, las tecnologías de la información, produciéndose así una informatización de los tipos tradicionales[137]. Por el contrario, los segundos constituyen nuevas conductas ilícitas donde el sistema informativo es el objeto de ataque, y que todavía no han encontrado su reflejo en el Código Penal en la mayoría de los casos, a diferencia de los anteriores.

En los sucesivos puntos analizaré aquellos ilícitos que, siendo objeto o medio, son los más usuales, pudiendo ser cualquiera de nosotros víctimas, tratando de analizar sus principales elementos para poder así identificarlos fácilmente y en consecuencia evitarlos o al menos prevenirlos.

2.1. DELITOS CONTRA LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE DATOS Y SISTEMAS INFORMÁTICOS

A. "HACKING": EL DENOMINADO INTRUSISMO INFORMÁTICO

El **hacking** es aquella conducta llevada a cabo en la Red, definida por E. MORÓN LERMA como "el conjunto de comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o red de comunicaciones y a la utilización de los mismos sin autorización o más allá de la misma"[138], siendo importante destacar que ésta conducta no se emprende con una finalidad destructiva o dañina, a diferencia del cracking.

---

[136] REZENDE CECILIO, Leonardo. Política criminal en el ciberespacio: critica al concepto de crimen informático. En: BUENO DE MATA, Federico. *Fodertics 3.0: (estudios sobre nuevas tecnologías y justicia).* Granada: Comares, 2015. ISBN: 978-84-9045-239-4. Pág.:225.

[137] (VELASCO SAN MARTÍN, Cristos. *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet.* Valencia: Tirant lo Blanch, 2012. ISBN: 978-84-9004-981-5. Pág.: 53).

[138] BARRIO ANDRÉS, Moisés. El régimen jurídico de los delitos cometidos en internet en el derecho español tras la reforma penal de 2010. En: *Delincuencia informática. Tiempos de cautela y amparo.* Cizur Menor (Navarra): Thomson Reuters Aranzadi, 2012. ISBN: 978-84-9014-273-8. Pág.: 40.

Por lo tanto, y derivado del término anterior, las personas encargadas de ejecutar esta maniobra son los **hackers**[139]**.** La ausencia de una acción destructiva en ellos determina una visión de los mismos "como sujeto inofensivo, que realiza una conducta inocua y carente de relevancia jurídico-penal alguna, como sujeto que ayuda al funcionamiento del sistema"[140], sin embargo, no todos llevan a cabo el intrusismo con un mismo móvil, permitiéndonos diferenciar tres tipos de hackers[141]:

- White Hat Hackers o Hackers de Sombrero Blanco: son los más benignos de entre los tres tipos, ya que "se especializan en realizar pruebas de penetración con el fin de asegurar que los sistemas de información y las redes de datos de las empresas"[142] son totalmente seguros, comunicando las debilidades encontradas de una manera completamente altruista.
- Black Hat Hackers o Hackers de Sombrero Negro: tiene como principal motivación el dinero, intentando conseguirlo vulnerando la seguridad de los sistemas con los métodos menos éticos posibles, siendo por ello lo más cercano a los crackers. Un ejemplo típico es el robo de información confidencial.
- Gray Hat Hackers o Hackers de Sombrero Gris: se encuentran a la deriva entre los dos anteriores, pudiendo actuar como los de sombrero blanco pero no de manera desinteresada, sino a cambio de una recompensa.

Refiriéndonos ahora al **método** que emplean para poder introducirse en el sistema, éste puede ir desde lo más sencillo y simple como **"**el acceso físico directo desde el propio ordenador de la víctima" por un despiste humano, pasando por el "control remoto de éste", hasta formas más complejas empleando "programas maliciosos[143] destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema"[144].

A pesar de ser una conducta llevada a cabo desde hace decenas de años, no fue hasta la entrada en vigor de la **Ley Orgánica 5/2010, de 22 de junio, por la que se modifica el Código Penal**, cuando el legislador tipifica esta conducta como hecho delictivo al introducirse en el artículo 197 un nuevo apartado 3[145], encargado de castigar tanto el acceso sin autorización a un sistema informático, como el mantenimiento en el mismo en contra de

[139] Denominado por el DRAE como "pirata informático": http://dle.rae.es/?id=JxlUKkm.

[140] MATELLANES RODÍGUEZ, Nuria. *Vías para la tipificación del acceso ilegal a los sistemas.* (http://www.uhu.es/revistapenal/index.php/penal/article/viewFile/362/353). [Fecha de consulta: 07-10-2016].

[141] SAN MIGUEL, Axel. *8 tipos de hackers que debes conocer.* (http://axelsanmiguel.com/8-tipos-de-hackers-que-debes-conocer/). [Fecha de consulta: 07-10-2016].

[142] DUARTE, Eugenio. *7 tipos de hackers y sus motivaciones.* (http://blog.capacityacademy.com/2012/07/11/7-tipos-de-hackers-y-sus-motivaciones/). [Fecha de consulta: 07-10-2016].

[143] Virus, troyanos, bombas lógicas, etc.

[144] A éstos métodos hace referencia: FERNANDEZ TERUELO, Javier Gustavo. *Derecho penal e internet: especial consideración de los delitos que afectan a jóvenes y adolescente.* Valladolid: Lex Nova, 2011. ISBN: 978-84-9898-365-4. Pág.:199.

[145] En la actualidad dicha regulación se localiza en el artículo 197 bis. 1 del CP: "El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".

la voluntad de quien tenga el legítimo derecho a excluirlo, a pesar de que en el pasado haya podido contar con su consentimiento. A mi juicio, esta regulación otorgada por el CP resulta insuficiente a la par que escueta, sin una redacción que nos permita diferenciar cuando un acceso se convierte en mantenimiento o qué tipo de consentimiento es válido para considerar que el intrusismo se lleva a cabo en contra de la voluntad de quien tiene legítimo derecho ante el sistema para excluirlo.

B. "CRACKING" O SABOTAJE INFORMÁTICO: LOS DAÑOS INFORMÁTICOS

Si antes hacíamos referían al hacking como medio para menoscabar la privacidad, el **cracking** está integrado por aquellos "comportamientos que van dirigidos a atacar los elementos lógicos del sistema, es decir, al software[146] en general y a los ficheros o archivos en los que se recogen datos, información, documentos electrónicos, cualquiera que sea su contenido en concreto"[147]. Por lo tanto, los daños pueden recaer tanto sobre el sistema informático en sí (por ejemplo, "mediante la alteración o corrupción de la programación favoreciendo la causación de errores aleatorios en el funcionamiento del sistema"[148]), como en la información de cualquier tipo contenida en él (destruyendo o modificando datos, programas informáticos, documentos, etc.), apartándonos del concepto tradicional de daño material.

Por lo tanto, un **cracker** "es alguien que viola la seguridad de un sistema informático para hacer daño de manera intencionada; elimina o borra ficheros, rompe los sistemas informáticos o introduce virus"[149]; es alguien que va más allá que los hackers, encontrando en ellos los fines destructivos inexistentes en la figura del apartado anterior.

De entre las distintas **modalidades comisivas** empleadas por estos sujetos para la producción de los daños podemos destacar, por su idoneidad y complejidad, los *malware* o *software* malicioso, los cuales consisten en "un conjunto de códigos y programas, que, introducidos en un sistema informático, originan problemas de utilización u operatividad de los mismos- de sus programas de funcionamiento- o alteración o borrado de datos", así como los ya tradicionales "*crash programs* o programas destructores (virus, gusanos, conejos, troyanos, etc.)"[150].

---

[146] Integrado por los componentes lógicos del sistema.

[147] GUDÍN RODRIGUEZ-MAGARIÑOS, Fausto. *Nuevos delitos informáticos: phising, pharming, hacking y cracking.* (http://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20informáticos.pdf) [Fecha de consulta: 10-10-2016].

[148] DE LA MATA BARRANCO, Norberto J., HERNÁNDEZ DÍAZ, Leyre. Los delitos vinculados a la informática en el Derecho Penal español. En: DE LA CUESTA ARZAMENDI, José Luís. Derecho penal informático. Madrid: Civitas, 2010. ISBN: 978-84-470-3429-1. Pág.: 162.

[149] FERNANDEZ TERUELO, Javier Gustavo. *Derecho penal e internet: especial consideración de los delitos que afectan a jóvenes y adolescente.* Valladolid: Lex Nova, 2011. ISBN: 978-84-9898-365-4. Pág.: 95.

[150] Ambas modalidades extraídas de: DE LA MATA BARRANCO, Norberto J., HERNÁNDEZ DÍAZ, Leyre. Un ejemplo de delitos informáticos: Delitos contra sistemas y datos en el Código Penal español ¿delitos de daños? En: DE LA CUESTA ARZAMENDI, José Luís. *Derecho penal informático.* Madrid: Civitas, 2010. ISBN: 978-84-470-3429-1. Pág.: 202.

Éstas conductas descritas también encuentran subsunción en el Código Penal a través del **artículo 264**, cuando el daño recaiga sobre datos informáticos, programas informáticos o documentos ajenos; y del **artículo 264 bis**., cuando el objetivo del ataque sea el sistema informático y su funcionamiento; siendo ambos delitos de resultado, "por cuanto requiere la producción de un resultado grave"[151], pero sin cuantificar el mismo en una cantidad concreta que facilite su aplicación. Así mismo nos encontramos "ante un tipo delictivo eminentemente doloso, donde debe acreditarse el propósito del autor de dañar los sistemas informáticos o sus componentes"[152].

2.2. CONDUCTAS FRAUDULENTAS COMETIDAS EN LA RED

A. EL PHISHING Y EL PHARMING: DEFINICIÓN Y MÉTODO OPERANDI

En ambos casos nos encontramos ante conductas fraudulentas encaminadas a la obtención tanto de los datos de usuario, como de las contraseñas correspondientes, pertenecientes a clientes de entidades bancarias con el objetivo de obtener transacciones ilícitas de dinero desde la cuenta de la víctima, siendo ésta quien, sin ser consciente de ello, hace llegar a los defraudadores la "llave" de sus cuentas bancarias. Éstas prácticas serian inimaginables sin la existencia de la banca online, puesto que usan Internet como vía para defraudar.

Sin embargo, a pesar de que ambas practicas persiguen la misma finalidad, su modus operandi es dispar.

- **El "phishing"**

  Como ya se puede ver reflejado en el título, la palabra phishing encuentra su **origen** en el vocablo ingles *fishing* (pescar), refiriéndose al intento de los defraudadores de pescar los datos y contraseñas de sus víctimas echando un anzuelo, aunque también se dice que en realidad "es la contracción de "*password harvesting fishing*" (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo"[153].

  El phishing ha sido **definido** por el APWG[154] "como un mecanismo que emplea tanto técnicas de ingeniería social y técnicas evasivas para robar la

[151] BARRIO ANDRÉS, Moisés. El régimen jurídico de los delitos cometidos en internet en el derecho español tras la reforma penal de 2010. En: *Delincuencia informática. Tiempos de cautela y amparo.* Cizur Menor (Navarra): Thomson Reuters Aranzadi, 2012. ISBN: 978-84-9014-273-8. Pág.: 44.
[152] SJP Nº1 Madrid de 29 julio 2005 (JUR 2006/70162), en su FJ Primero.
[153] SAPENE CISNEROS, Juan Enrique. *Phishing ¿Qué es? ¿Cómo lo hacen? ¿Cómo evitarlo?*. (https://www.digitalconexion.com/newsite/Phishing-Que-es-Como-lo-hacen-Como-evitarlo.html). [Fecha de consulta: 11-10-2016].
[154] Iniciales de Anti-Phising Working Group

identidad, los datos personales y la información financiera de los consumidores"[155], o de una manera más sencilla y en palabras de nuestro Tribunal Supremo[156], se tratan de estafas en las que a través de artificios informáticos desconocidos la presunta o presuntos autores realizan disposiciones patrimoniales no consentidas.

El **método** empleado por los *phiser* para apoderarse del patrimonio de sus víctimas, consiste en el envío indiscriminado de correos electrónicos a usuarios de bancas electrónicas. Estos correos suelen contener enlaces de páginas web falsas a las cuales les redirigen, contando tanto ésta como los correos con un interfaz idéntico al de la entidad bancaria de la que es cliente la víctima ya que "aparece una imitación de la cabecera del mensaje como si fuera la entidad bancaria del usuario, incluso utiliza mismos logos y mismos símbolos, pidiendo al usuario que renueve sus claves de acceso introduciéndolas en los aparatos dispuestos para ello"[157]. Una vez obtenidas las claves, "realiza con ellas operaciones en la Red, normalmente transferencias bancarias o compras inconsentidas e ignoradas a través de Internet, y a veces también retirada de efectivo en cajeros o duplicado de tarjetas con esos fines"[158].

Hoy en día, en lugar de mandar miles de mensajes a personas aleatorias, está en auge la técnica conocida como ***spear-phishing,*** consistente en "mandar mensajes estafa a objetivos concretos, bien sea un grupo de trabajadores de una misma empresa, bien sea una única persona, consiguiendo tasas de éxito 10 o 100 veces mayores: se estudian sus hábitos y se crea mensajes a medida"[159]. Por lo tanto, a pesar de desplegar el engaño ante menos usuarios, su tasa de éxito es mayor al diseñar a medida los correos electrónicos que se les remite en función de sus gustos o intereses.

También existen otras posibles variantes como el ***smishing***[160], donde el fraude se comete vía SMS al teléfono móvil, o el ***vishing***[161] con las llamadas de teléfono como protagonistas.

---

[155] VELASCO SAN MARTÍN, Cristos. *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet.* Valencia: Tirant lo Blanch, 2012. ISBN: 978-84-9004-981-5. Pág.: 71.

[156] En **TS, auto de 12 noviembre 2009 (JUR 2009/474656), FJ Segundo.**

[157] Autor desconocido. *Calificación jurídica del mulero en el phising.* (http://es.slideshare.net/rafameca/calificacin-jurdica-del-mulero-en-el-phising). [Fecha de consulta:11-10-2016].

[158] VELASCO NÚÑEZ, Eloy. *Los delitos informáticos: la reparación y las indemnizaciones. Especial referencia al fraude.* (http://www.elderecho.com/tribuna/penal/informaticos-reparacion-indemnizaciones-Especial-referencia_11_194680019.html). [Fecha de consulta: 11-10-2016].

[159] MEDINA LINÀS, Manel. *Cibercrimen: ¡protégete del "bit-bang"!, los ataques en el ciberespacio a tu ordenador, tu móvil, tu empresa: aprende de víctimas, expertos y cibervigilantes.* Barcelona: Tibidabo, 2015. ISBN: 978-84-16204-82-3. Pág.: 33.

[160] REY HUIDOBRO, Luis Fernando. *La estafa informática: relevancia penal del phising y el pharming.* (http://www.bufetelineros.eu/es/noticia.asp?pag=&id=2491&por=1). [Fecha de consulta: 12-10-2016].

[161] RODRIGUEZ CARO, María Victoria. Estafa informática. *El denominado phishing y la conducta del "mulero bancario": categorización y doctrina de la Sala Segunda del Tribunal Supremo.* (http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo%3Bmulero/). [Fecha de consulta:12-10-2016].

Antes de finalizar con el phishing, me parece interesante analizar una figura que cobra especial importancia en toda esta trama, y especialmente en aquellos casos en los que tienen lugar elevadas transferencias de dinero. Éstas figuras son los **muleros o *"phishing-mules",*** y son los encargados de llevar a cabo una "conducta de colaboración que opera con posterioridad a la consumación de la defraudación patrimonial"[162], abriendo cuentas a su nombre[163] a las que posteriormente se les transfiere parte de las cantidades que han sido defraudadas por los phiser, a cambio de una comisión.

El primer gran caso de fraude a una entidad bancaria siguiendo este método tuvo lugar en 1994, fue llevado a cabo por Vladimir Levin y la víctima en este caso fue el banco CiItibank [164].

- **El "pharming": una granja de servidores**

El **origen** de ésta palabra lo encontramos en el término inglés *"farm"* (granja), para referirse a la situación en la que, "una vez que el atacante ha conseguido acceso a un servidor DNS o varios servidores (granja de servidores o DNS), se dice que ha hecho un pharming"[165]. Por lo tanto, tiene a su disposición un abanico de servidores de los que puede hacer uso para defraudar.

El pharming puede ser **definido** como la "explotación de una vulnerabilidad en el software de los servidores DNS[166] *(Domain Name System)* o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio *(domain name)* a otro ordenador diferente"[167]. De esta manera, una vez que el defraudador consigue acceder al servidor DNS de su víctima, puede tomar el control de éste y redirigirla a la página que él desee.

Por lo tanto, esta práctica puede ser considerada como un tipo de phishing por su finalidad, pero en este caso no hay nadie que se ponga en contacto con la victima a través de correos electrónicos, SMS o llamada telefónicas. **El modo operandi** del pharming comienza con la creación de páginas webs encargadas de

---

[162] OXMAN VILCHES, Nicolás André. *Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"*. (http://www.scielo.cl/pdf/rdpucv/n41/a07.pdf). [Fecha de consulta: 12-10-2016].

[163] Denominadas cuentas "nido" o cuentas "puente".

[164] Más sobre este caso en: MEDINA LINÀS, Manel. *Cibercrimen: ¡protégete del "bit-bang"!, los ataques en el ciberespacio a tu ordenador, tu móvil, tu empresa: aprende de víctimas, expertos y cibervigilantes.* Barcelona: Tibidabo, 2015. ISBN: 978-84-16204-82-3. Pág.: 30.

[165] TABUENCA, Alex. *El cortafuego: phishing y pharming.* (http://elcortafuegosdeinternet.blogspot.com.es/2010/06/phising-y-pharming.html). [Fecha de consulta: 12-10-2016].

[166] Son los encargados de conducir a los usuarios a la página web que desean ver.

[167] GUDÍN RODIGUEZ-MAGARIÑOS, Faustino. La lucha contra el ciberblanqueo como vía para acabar con el pishing. *Revista Aranzadi Doctrinal.* 2014, Nº. Extra 9-10, págs. 261-293. ISSN: 1889-4380.

simular aquellas a las cuales la victima realmente quiere acceder (normalmente páginas web de banca online), y que contienen el fraude. Posteriormente tiene lugar la manipulación de las direcciones DNS utilizadas por el usuario, de manera que "mecánicamente le conducen a éste cuando las escribe en el navegador de Internet a páginas que no son la deseada, aunque aparentemente presentan un aspecto idéntico"[168]. Una vez han sido reenviados a la página web falsa, introducen en ella los datos confidenciales que directamente llegan a manos de los delincuentes, llevando a cabo con ellas las mismas acciones que han sido expuestas en el punto anterior.

B. LOS ARCHIVOS ESPÍA COMO MEDIO PARA SUSTRAER LAS CLAVES

Si en el punto anterior se han analizado fraudes patrimoniales en los cuales es la víctima quien se dirige al defraudador y le concede de manera inconsciente sus datos confidenciales, en estos casos va a ser el defraudador quien va a ir hasta la víctima, accediendo a su ordenador, para "robar" sus datos de las tarjetas de crédito, las claves de acceso a la página web de su banco, etc.

El acceso a los ordenadores tiene lugar a través de diversos tipos de ***malware*** (del inglés *malicious software*) o ***software malicioso.*** Éstos, son "programas de cómputo que son introducidos en los sistemas de información de los usuarios para causarles algún daño o simplemente para modificar su uso y obtener su control"[169], por lo que, además de ser capaces de provocar daños en los sistemas informáticos como ya hemos visto en el punto correspondiente, también pueden ser empleados para recoger datos personales del usuario y enviarlos a terceras personas sin que sean conscientes de ello.

Dentro del término malware se incluyen una pluralidad de figuras tales como virus, conejos o bacterias, gusanos, troyanos, bombas lógicas, backdoors, etc. Sin embargo, existen tres tipos de malware que destacan por su idoneidad para la sustracción de claves y datos personales:

- **Spyware o software espía**

  Los spyware son "programas de software espía que tienen la capacidad de auto-instalarse en las computadoras personales de los usuarios, con objeto de conocer su identidad y monitorear su comportamiento al usar sistemas de cómputo o navegar en Internet, siendo capaz de crear bases de datos y proporcionar

[168] VELASCO NÚÑEZ, Eloy. *Los delitos informáticos: la reparación y las indemnizaciones. Especial referencia al fraude.* (http://www.elderecho.com/tribuna/penal/informaticos-reparacion-indemnizaciones-Especial-referencia_11_194680019.html). [Fecha de consulta: 12-10-2016].

[169] VELASCO SAN MARTÍN, Cristos. *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet.* Valencia: Tirant lo Blanch, 2012. ISBN: 978-84-9004-981-5. Pág.: 73.

información y updates sobre las preferencias y hábitos personales de los usuarios"[170].

Estos programas pueden llegar hasta nuestro ordenador a través de enlaces que lo instalan y que se ejecutan al hacer click sobre un cuadro de dialogo engañoso emergente en una página web, o puede venir incluido en otro software que instalamos intencionadamente[171].

Una vez han recopilado los datos perseguidos, son enviados desde el propio ordenador de la víctima, al ordenador del defraudador.

- **Scareware: el programa que se aprovecha del miedo**

El scareware "es un tipo de programa maligno que se vende empleando prácticas de publicidad engañosa y antiética, usualmente recurriendo a amenazas inexistentes"[172]. La manera más usual en la que se introduce en el ordenador es mediante "pop-ups que afirman que un virus ha atacado nuestro sistema. Esta amenaza es cierta, pero no del modo que sugieren dichos pop-ups. Estos, después, nos obligan a descargarnos varias aplicaciones de seguridad que eliminan los supuestos virus. Normalmente, esas descargas son el escondite para el malware"[173].

- **Keyloggers: el registrador de teclas**

Un keylogger es un "programa capturador de las teclas pulsadas, introducido de forma maliciosa, con el que el defraudador puede hacerse con las claves aun cuando se envíen de forma cifrada, pues permite identificar todas las teclas que se han pulsado durante el proceso de acceso telemático a la entidad"[174]. Con la finalidad de minimizar los efectos de estos softwares maliciosos, gran parte de las entidades bancarias han instaurado en sus páginas webs, teclados virtuales que evitan al usuario tener que teclear sus datos y contraseñas, por lo que su uso es más que recomendado.

---

[170] VELASCO SAN MARTÍN, Cristos, JIMÉNEZ ROJAS, Jesús Ramón. *Spyware, el software espía.* (http://www.enterate.unam.mx/Articulos/2005/marzo/spyware.htm). [Fecha de consulta: 12-10-2016].

[171] Ver: TENZER, Simón Mario. *Riesgo Informático: "Spyware", "Adware" y "Popup"*. (http://www.ccee.edu.uy/ensenian/catcomp/material/Inform %20II/SPYWARE.PDF). [Fecha de consulta: 12-10-2016].

[172] LÓPEZ AZAMAR, Bertha. *Software malintencionado e infeccioso.* (http://www.unpa.edu.mx/~blopez/Computacion/complementario/VirusYotrosMalware.pdf). [Fecha de consulta: 12-10-2016].

[173] MALENKOVICH, Serge. *7 pasos para recuperarnos del Scareware.* (https://blog.kaspersky.es/7-pasos-para-recuperarnos-del-scareware/165/). Fecha de consulta: 12-10-2016].

[174] CRUZ RIVERO, Diego. La suplantación de identidad en el ámbito electrónico y la defraudación de la banca electrónica. *Revista de derecho bancario y bursátil.* 2010, Nº 117, págs. 191-230. ISSN: 0211-6138.

C. SUBSUNCIÓN DE ESTAS CONDUCTAS EN NUESTRO CÓDIGO PENAL

Estas prácticas se encuentran tipificadas en nuestro CP dentro del Título XIII, encargado de regular los "Delitos contra el patrimonio y contra el orden socioeconómico". Concretamente, es el **artículo 248 en su apartado 2 a)** el destinado a castigar estos comportamientos con la siguiente redacción: "También se consideran reos de estafa los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro".

El mencionado artículo fue introducido en el texto original de 1995 como un nuevo tipo de estafa, diferenciada de la tradicional, con el principal objetivo de "sancionar situaciones fraudulentas planteadas en entidades bancarias o terminales de pago (TPV) en las que algún empleado o tercero operando sobre ellas, realizaba transferencias a su favor o a favor de tercero"[175]. Sin embargo en la actualidad, también abarca todas las actuaciones descritas en los apartados A) y B) del presente trabajo.

Por el contrario, éstas no podrían considerarse encuadradas dentro de la estafa clásica o tradicional, ya que en estos casos el estafador no provoca en la victima, engaño bastante que dé lugar a error. Así lo ha considerado nuestro **Tribunal Supremo en su sentencia núm. 2175/2001**[176], al considerar que "el engaño, propio de la relación personal, es sustituido como medio comisivo defraudatorio, por la manipulación informática o artificio semejante en el que lo relevante es que la máquina, informática o mecánica, actúe a impulsos de una actuación ilegítima".

2.3. CONDUCTAS QUE AFECTAN A PERSONAS ESPECIALMENTE VULNERABLES

Hoy en día los menores de edad se ven expuestos a peligros que hace años parecían inimaginables. El acceso de la mayor parte ellos a teléfonos móviles de última generación con conexión a Internet[177], la proliferación de redes sociales tales como Facebook, Twitter, WhatsApp, Snapchat, etc., hacen que tanto la comunicación entre ellos como el intercambio de contenidos multimedia estén a su disposición con un solo click. A pesar de que nuestros jóvenes, ya conocidos bajo el seudónimo de "nativos digitales"[178], poseen amplios conocimientos en las denominadas TIC's, su escasa edad hace que muchas veces no sean

[175] FERNANDEZ TERUELO, Javier Gustavo. *Derecho penal e internet: especial consideración de los delitos que afectan a jóvenes y adolescente.* Valladolid: Lex Nova, 2011. ISBN: 978-84-9898-365-4. Pág.: 46.
[176] **STS 20 noviembre 2001 (RJ 2002\805), en su FJ Primero.**
[177] Según datos del INE, el 69,8% de los niños de 10 a 15 años disponen de un teléfono móvil; un 95,2 % han sido usuarios de Internet en los últimos 3 meses, y un 94,9% han sido usuarios de un ordenador en los últimos 3 meses. Fuente: (http://www.ine.es/jaxi/Datos.htm?path=/t25/p450/base_2011/a2016/l0/&file=01005.px).
[178] LORENTE LÓPEZ, María Cristina. La vulneración de los derechos al honor, a la intimidad y a la propia imagen de los menores a través de las Nuevas Tecnologías. *Revista Aranzadi Doctrinal.* 2015, Nº 2, págs..: 201-222. ISSN: 1889-4380.

capaces de discernir el riesgo que conlleva determinadas actuaciones llevadas a cabo por ellos mismos en la Red.

El uso inadecuado de la tecnología que tienen en su poder, unido a la menor concienciación de los peligros que los rodean, hace que los menores de edad vean quebrantados sus derechos más elementales en diversas situaciones que a continuación analizaré.

A. SEXTING Y SEXTORSIÓN

La palabra sexting tiene su **origen** en la combinación de palabras anglosajonas, y "trata de reflejar sintéticamente la fusión entre sexo (sex) y mensajes vía móvil (texting)"[179].

De una manera comprensible puede **definirse** como el envío, en este caso por parte de menores, de mensajes consistentes en textos, imágenes o vídeos, caracterizados por su alto contenido sexual, de una manera voluntaria y a través de dispositivos tecnológicos. Por lo tanto, sus cuatro elementos principales son los siguientes[180]:

- La voluntariedad en los actos
- La utilización de dispositivos tecnológicos
- El carácter sexual o erótico de los contenidos
- Naturaleza privada y casera de los contenidos

En muchas ocasiones ésta práctica no tiene por qué originar una conducta delictiva, pudiendo poner el ejemplo de dos adolescentes que deciden intercambiarse imágenes con contenido sexual voluntariamente. Sin embargo, pueden surgir diversos problemas si el uso que se da a los mensajes, una vez han sido recibidos, no es el correcto.

En primer lugar, puede ocurrir que el receptor de las imágenes decida **distribuirlas** en contra de la voluntad de quien se las envió, menoscabando su honor, su intimidad, su vida privada, su dignidad, etc. A pesar de que el texto original del CP no recogía estos supuestos[181], en la última modificación del mismo llevada a cabo por la LO 1/2015, de 30 de marzo, el legislador decir tipificar como delito estas conductas en el **artículo 197.7**[182].

---

[179] FLORES FERNÁNDES, Jorge. *Sexting: adolescentes, sexo y teléfonos móviles.* (http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/pdfs/pantallasamigas-sexting-adolescentes-sexo-y-telefonos-moviles.pdf). [Fecha de consulta: 13-10-2016].

[180] ANAYANSSI ORIZAGA, Isabel. ENOE CABRERA, Karen. Sexing y redes sociales: diversas relaciones y consecuencias jurídicas. En: BUENO DE MATA, Federico. *Fodertics 3.0: (estudios sobre nuevas tecnologías y justicia).* Granada: Comares, 2015. Págs.: 186-196. ISBN: 978-84-9045-239-4. Pág.:188.

[181] Únicamente penalizaba el apoderamiento de imágenes sin consentimiento para descubrir secretos o vulnerar la intimidad del otro, por vía del artículo 197.1.

[182] "Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona".

En segundo lugar, el receptor de los mensajes sexuales puede decidir utilizarlos en contra del emisor con la finalidad de conseguir algo a cambio (por ejemplo, más imágenes de la misma connotación o una cantidad de dinero), empleando para ello la persuasión o chantaje. Estos casos son conocidos bajo el nombre de **sextorsión**, consistente en "la amenaza de difundir la imagen o grabación, con contenido sexual o erótico, previamente obtenida, normalmente con consentimiento de la víctima, si no realiza aquello que el poseedor de las imágenes le exige"[183]. Por el momento no existe en nuestro Código Penal un tipo propio encargado de regular esta situación, "debiendo reconducirse a otros tipos penales como la extorsión o el chantaje, según el caso concreto"[184].

B. EL CHILD GROOMING O PROPUESTA SEXUAL TELEMÁTICA A MENORES

Al igual que cada uno de nosotros nos hemos ido adaptando y sacando el mejor partido a las nuevas tecnologías, los delincuentes sexuales también se han adaptado a los ámbitos en los que se mueven sus víctimas en los últimos tiempos. Esto ha provocado que los encuentros a las salidas de colegios, o los acercamientos "casuales" en parques se hayan visto reemplazados por la creación de perfiles en redes sociales, en la mayoría de los casos falsos, o la participación en chats donde a menudo se mueven los más jóvenes, con la finalidad de contactar con menores y ganarse su confianza.

Para poder ir entendiendo lo que significa el child grooming, debemos acudir a la expresión en inglés ***«to groom somebody for something»*****,** que unido a su significado original (*to groom*: acicarlarse) nos da las claves para conocer esta conducta, por la cual "una persona se metamorfosea para iniciar una línea seductora de comportamiento orientado a la captación de una voluntad, aún no formada"[185].

Siguiendo la línea anterior, el child grooming pude ser **definido** como una práctica por la cual "un adulto (generalmente un depredador sexual) contacta con un menor a través de redes sociales o valiéndose de Internet para crear un vínculo afectivo, intentando ganarse la confianza del mismo, para concertar una cita con claros fines sexuales"[186].

Dentro del proceso de acercamiento al menor protagonizado por el *groomer,* podemos distinguir seis fases[187]:

---

[183] DOMINGUEZ MATEOS, Isabel. ESTEBAN RUIZ, Adaya María. GARCÍA DE PABLOS, María. Sextorsión: Tortura en la Red. En: BUENO DE MATA, Federico. *Fodertics 4.0: (estudios sobre nuevas tecnologías y justicia).* Granada: Comares, 2015. Págs.: 155-162. ISBN: 978-84-9045-274-5. Pág.:156.

[184] GUARDIOLA SALMERÓN, Miriam. *El "sexteo", el "sexting" y la "sextorsión".* (http://www.lawandtrends.com/noticias/penal/el-sexteo-el-sexting-y-la-sextorsion.html). [Fecha de consulta: 13-10-2016].

[185] GUDÍN RODRIGUEZ-MAGARIÑOS, Faustino. Algunas consideraciones sobre el nuevo delito de Grooming. En: *Delincuencia informática. Tiempos de cautela y amparo.* Cizur Menor (Navarra): Thomson Reuters Aranzadi, 2012. Págs.: 141-149. ISBN: 978-84-9014-273-8. Pág.: 141.

[186] BIURRUN ABAN, Fernando J. Los riesgos de las nuevas tecnologías. *Actualidad jurídica Aranzadi.* 2016, Nº 921, pág.: 28. ISSN 1132-0257.

[187] Extraídas y desarrolladas extensamente en: VILLACAMPA ESTIARTE, Carolina. *El delito de "online child grooming" o propuesta sexual telemática a menores.* Valencia: Tirant lo Blanch, 2015. ISBN: 978-84-9086-445-6. Págs.: 32-35.

1. Selección de su víctima: el delincuente elige al menor, por ejemplo, mediante la visualizando de perfiles en redes sociales o manteniendo conversaciones en chats con temáticas adaptadas a su edad.
2. Fase de establecimiento de amistad: únicamente con la intención de conocer al niño y obtener alguna foto suya si connotaciones sexuales.
3. Fase de conformación de la relación: afianza su amistad con el menor haciéndose pasar por un verdadero amigo, ganándose por completo su confianza.
4. Fase de valoración de riesgo: en esta fase el *groomer* trata de averiguar si existe peligro de que sus actuaciones puedan llegar a ser conocidas por las personas encargadas del cuidado del menor.
5. Fase de exclusividad: en ella la relación es más personal y comienzan a aparecer ciertas situaciones con matices sexuales, por ejemplo, mediante preguntas "inocentes".
6. Fase sexual: en la fase final se pasan de conversaciones donde el aspecto sexual se encuentra implícito, a intercambios explícitos acompañados, en la mayoría de los casos, del intercambio de materia pornográfico incluso del menor.

Eventualmente, puede surgir la fase conocida como ***cyber stalking***, que tiene lugar cuando "aparece la negativa del menor a mantener el contacto con el acosador, advirtiendo al menor de que se lo comunicara a sus padres y a sus amigos[188]" con el objetivo de intimidarle y que continúe con la relación creada entre ambos.

La importancia de prevenir y atacar estas conductas radica en el carácter de acto preparatorio que posee respecto a otras más graves como la tenencia y divulgación de material pornográfico, supuestos de cyberbulling e incluso abusos sexuales. En este ámbito de prevención y formación cabe destacar el proyecto Ciberexpert@[189], encargado, ente otras acciones, de impartir charlas en aquellos centros educativos que lo soliciten de manera voluntaria con el fin de informar a los alumnos de diversos peligros como el aquí expuesto.

En nuestro país el CP recoge en su **artículo 183 ter 1.** el tipo penal más próximo al child grooming, introducido por la LO 5/2010, de 22 de junio, y modificado posteriormente por la LO 1/2015, de 30 de marzo, configurándose como un "tipo de mera actividad al ser suficiente la mera oferta para concretar un encuentro, sin que se exija un resultado"[190].

[188] LORENTE LÓPEZ, María Cristina. La vulneración de los derechos al honor, a la intimidad y a la propia imagen de los menores a través de las Nuevas Tecnologías. *Revista Aranzadi Doctrinal.* 2015, Nº 2, págs..: 201-222. ISSN: 1889-4380.

[189] Sobre este proyecto se hace eco la noticia: TORRES, Mònica. *La policía quiere que los niños sean Ciberexpert@s.* (http://elpais.com/elpais/2016/06/02/actualidad/1464875428_167957.html). [Fecha de *consulta*: 14-10-16].

[190] GUDÍN RODRIGUEZ-MAGARIÑOS, Faustino. Algunas consideraciones sobre el nuevo delito de Grooming. En: *Delincuencia informática. Tiempos de cautela y amparo.* Cizur Menor (Navarra): Thomson Reuters Aranzadi, 2012. Págs.: 141-149. ISBN: 978-84-9014-273-8. Pág.: 144.

C. CYBERBULLYING: ACOSO EN LA RED

El ***cyberbullying***, derivado del tradicional *bullying* o acoso escolar, consiste en "el uso de los medios telemáticos (Internet, telefonía móvil y videojuegos online principalmente) para ejercer el acoso psicológico entre iguales"[191], siendo el principal objeto de ataque la dignidad de la víctima. En este punto se deben descartar tanto los acosos de índole estrictamente sexual, como aquellos en los que intervienen adultos y las meras acciones puntuales.

A diferencia de lo ocurrido en el *bullying*, el contacto no es directo por lo que no entran en juego lesiones físicas. Sin embargo, el acoso puede producirse las 24 horas del día y además su contenido es mucho más difícil de controlar al expandirse por la Red de una manera rápida y difícil de borrar. Esto hace del *cyberbullying* un problema no menos grave.

A pesar de que las **formas** en las que el cyberbullying se puede manifestar son muy variadas, de manera resumida pueden agruparse en tres tipos[192]:

1. Acosando a través de Internet, como se haría en la vida real pero usando medios digitales para amenazar, chantajear, insultar, etc.
2. Usando Internet para difundir mensajes de escarnio o ridiculización a nuestros contactos, siendo el equivalente al tradicional "cotilleo".
3. Generando y distribuyendo información falsa sobre nosotros o nuestras actividades, suplantando nuestra identidad para ello o utilizando otra identidad real o falsa. Este comportamiento es conocido bajo el nombre de "cibercalumnia".

Desde un punto de vista procesal, en nuestro sistema jurídico existen dos vías posibles a las cuales se puede acudir en busca de tutela judicial en caso de sufrir *cyberbullying*:

- Vía penal: ya que en la actualidad no existe ningún tipo penal concreto que castigue este tipo de acoso, se deberá estudiar cada caso concreto para poder subsumirlo en el artículo correcto, en función de si lo que prima es el descubrimiento y revelación de secretos, el ataque a la integridad moral de menor, amenazas, coacciones, injurias, etc.
- Vía civil: se acude a ella "al amparo de la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen"[193].

---

[191] FLORES FERNÁNDEZ, Jorge. *Ciberbullying. Guía rápida.* (http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/pdfs/pantallasamigas-ciberbullying-guia-rapida.pdf). [Fecha de consulta: 14-10-2016].

[192] Extraídas de: MEDINA LINÀS, Manel. *Cibercrimen: ¡protégete del "bit-bang"!, los ataques en el ciberespacio a tu ordenador, tu móvil, tu empresa: aprende de víctimas, expertos y cibervigilantes.* Barcelona: Tibidabo, 2015. ISBN: 978-84-16204-82-3. Págs.: 124 y 125.

CONCLUSIONES

1.- Sobre las diligencias de investigación tecnológica

Con la LO 13/2015, de 5 de octubre, el legislador pone fin a una carente legislación española en esta materia, habiendo llegado a ser objeto de diversos pronunciamientos emitidos por el TEDH en los que se ponía de manifiesto el deseo de una modificación legislativa con la que se incorporara a la Ley, los principios que se desprenden de la jurisprudencia del mismo.

A pesar de que esta regulación resulta bastante completa al fijar una limitación al ámbito objetivo de cada una de ellas, y regular aspectos como su duración, el control judicial al que deben estar sometidas, o la posibilidad de prórroga de las mismas, la Ley deja a un lado cuestiones prácticas, como poder ser haber hecho mención a cuáles son los posibles instrumentos con los que realizar las diferentes diligencias, habiéndose remitido, en su lugar, a los "dispositivos técnicos" de una manera generalista. A su vez habría resultado útil la puntualización en cada una de las medidas, de aquellas posibles excepciones a la exigencia de autorización judicial, como puede suceder en la obtención de la numeración IMEI o IMSI, o por muy evidente que parezca, cuando medie el consentimiento del sujeto afectado.

Es en esta vertiente práctica, donde cobran especial interés las resoluciones dictadas por nuestros Tribunales, con anterioridad a la reforma, por ofrecer soluciones a supuestos concretos que la Ley no se para a descifrar.

Por lo tanto, la Jurisprudencia se presenta en esta materia como un complemento a la regulación ofrecida por la LO 13/2015, y ésta se encarga de poner fin a las distintas controversias doctrinales surgidas a lo largo de los años en torno a las diligencias de investigación tecnológica y sus presupuestos.

En definitiva, podemos afirmar que con esta reciente reforma se está dando un paso más hacia la aceptación de la revolución que las nuevas tecnologías están causando no solo en nuestro día a día, sino también en el Derecho.

2.- Sobre la prueba electrónica

El continuo avance tecnológico que está experimentando la sociedad, hace que podamos hablar de una necesidad imperiosa respecto a la elaboración de una normativa nacional, que se encargue de regular de una manera global la prueba electrónica, acabando así con las disputas doctrinales que han surgido en torno a cada uno de los puntos que

[193] LORENTE LÓPEZ, María Cristina. La vulneración de los derechos al honor, a la intimidad y a la propia imagen de los menores a través de las Nuevas Tecnologías. *Revista Aranzadi Doctrinal.* 2015, Nº 2, págs..: 201-222. ISSN: 1889-4380.

examinamos de ella, fijando así unos criterios que faciliten tanto su aportación en los distintos procedimientos judiciales, como la tarea de nuestros órganos enjuiciadores a la hora de poder valorarlas. Ésta exigencia responde a la gran utilidad que se puede extraer de la misma debido a la presencia cada vez más latente de las TIC's en prácticamente todos los ámbitos de la vida cotidiana de las personas.

Sin embargo, no solo es necesario una normativa nacional, sino también un esfuerzo por actualizarse y abrirse a una nueva perspectiva del Derecho en general, y procesal en particular. Así mismo esta nueva vertiente probatoria requiere de una formación judicial especifica por parte de, no sólo los cuerpos de seguridad sino también de los jueces, al ser ellos quienes tienen encomendada la tarea de apreciarla, valorarla, y estudiarla para poder enjuiciar de una manera justa.

Descartada su consideración como un nuevo medio probatorio, la prueba electrónica deberá ser aportada al proceso a través de algunos de los medios de prueba tradicionales: como prueba testifical, convirtiendo la prueba electrónica concreta en el centro del interrogatorio; como prueba documental trasladando la prueba en un documento electrónico (ej.: pantallazos de Whatsapp, SMS, correos electrónicos, comentarios registrados en redes sociales); mediante dictamen pericial, bien a instancia de parte o de oficio por decisión del Juez, en aquellos casos que se requiera de algún conocimiento informático especial; sometiéndola a reconocimiento judicial; o, dependiendo del soporte en el que la prueba se encuentre alojada, mediante la reproducción de la misma ante el Tribunal.

Una vez aportadas al proceso, ésta novedosa fuente de prueba tendrá la misma fuerza probatoria que las tradicionales.

3.- Sobre los delitos informáticos

Un acceso a Internet, así como a dispositivos electrónicos de todo tipo, cada día más factible para el conjunto de la población sin distinción de edad, sexo o incluso clase social, hace que día a día los casos y tipos de delitos informáticos aumenten considerablemente. Todo ello, unido a una exposición cada vez más descontrolada e inconsciente de los más jóvenes, hace que éstos se estén convirtiendo en uno de los principales objetivos de los ataques cibernéticos con las graves consecuencias que implica. Por ello es importante la puesta en marcha de las siguientes medidas:

- En lo que se refiere a los más jóvenes, se debe dar importancia a la formación e información sobre estos fenómenos como una parte más de su educación, haciendo especial hincapié en el riesgo al que se ven expuestos debido a su temprana edad, los principales indicios con los que pueden identificar alguno de los ilícitos estudiados, así como medidas para prevenirlos. Sería conveniente, así mismo, que esta formación se llegara a extender a toda la población, adaptándola según las circunstancias, pudiendo poner como ejemplo la

impartición de cursos en Universidades, centros de trabajo, o empleando los medios de comunicación como principal aliado.

- Desde un punto de vista penal, son necesarios tipos delictivos que se ajusten a esta nueva forma de delinquir, ya que, aunque algunos delitos como el hacking o el cracking ya cuentan con una regulación bastante acorde en nuestro CP, mientras que otros tan habituales y preocupantes como la sextorsión no cuentan aún con un tipo propio encargado de regular esta situación.

Por lo tanto, de poco vale una nueva regulación que otorgue la debida habilitación legal a los cuerpos de seguridad para llevar a cabo las diligencias de investigación destinadas a la averiguación de este tipo de delitos, si posteriormente, tras la fase probatoria no se consigue una pena específica y proporcional al tipo cometido.

En definitiva, es innegable que estos tres elementos analizados a lo largo del trabajo van de la mano, pues con la concesión de pruebas electrónicas gracias a la práctica de las diferentes diligencias de investigación tecnológica, las Fuerzas y Cuerpos de Seguridad del Estado conseguirán hacer frente, o al menos reducir, la cara negativa de las TIC's que están haciendo proliferar numerosos supuestos de delitos informáticos.

BIBLIOGRAFIA

ABEL LLUNCH, Xavier, PICÓ I JUNOY, Joan, et al. *La prueba electrónica.* Barcelona: Bosch, 2011. ISBN: 978-84-7698-955-5.

ANAYANSSI ORIZAGA, Isabel. ENOE CABRERA, Karen. Sexing y redes sociales: diversas relaciones y consecuencias jurídicas. En: BUENO DE MATA, *Federico. Fodertics 3.0: (estudios sobre nuevas tecnologías y justicia).* Granada: Comares, 2015. Págs.: 186-196. ISBN: 978-84-9045-239-4.

ARAZI, Roland. *La prueba en el proceso civil*. Buenos Aires: La Roca, 1998. ISBN: 950-9714-97-6.

ARIZA CLMENAREJO, María Jesús. La utilización de drones como herramienta en la investigación penal. En: BUENO DE MATA, Federico. *Fodertics 4.0: (estudios sobre nuevas tecnologías y justicia)*. Granada: Comares, 2015. Págs.: 107-116. ISBN: 978-84-9045-274-5.

BARRIO ANDRÉS, Moisés. El régimen jurídico de los delitos cometidos en internet en el derecho español tras la reforma penal de 2010. En: *Delincuencia informática. Tiempos de cautela y amparo.* Cizur Menor (Navarra): Thomson Reuters Aranzadi, 2012. ISBN: 978-84-9014-273-8.

BIURRUN ABAN, Fernando J. Los riesgos de las nuevas tecnologías. *Actualidad jurídica Aranzadi*. 2016, Nº 921, pág.: 28. ISSN 1132-0257.

BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0.* Valencia: Tirant lo Blanch, 2014. 978-84-9053-483-0.

BUENO DE MATA, Federico. Comentarios críticos a la inclusión de la figura del agente encubierto virtual en la LO 13/2015. En: En: BUENO DE MATA, Federico. *Fodertics 4.0: (estudios sobre nuevas tecnologías y justicia).* Granada: Comares, 2015. Págs.: 117-123. ISBN: 978-84-9045-274-5.

BUENO DE MATA, Federico. El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia. En: PÉREZ-CRUZ MARTÍN, Agustín-J. FERRREIRO BAAMONDE, Xulio. NEIRA PENA, Ana María. *Los retos del Poder Judicial ante la sociedad globalizada.* A Coruña: Universidade da Coruña, 2012. Págs.: 295-306. ISBN**:** 978-84-9749-501-1.

BUJOSA VADELL, Lorenzo M. La valoración de la prueba electrónica. BUENO DE MATA, Federico. *Fodertics 3.0: (estudios sobre nuevas tecnologías y justicia).* Granada: Comares, 2015. ISBN: 978-84-9045-239-4.

CAMPANER MUÑOZ, Jaime. ¿*Remore Forensic Software* en España? Acerca de la utilización de virus con fines de investigación en el proceso penal. En: BUENO DE MATA, Federico. *Fodertics II: hacia una justicia 2.0.* Salamanca: Ratio Legis, D.L. 2014. Págs.: 107-112. ISBN: 978-84-9045-274-5. Pág.:108.

CARNELUTTI, Francesco. *La prueba civil.* Buenos Aires: Arayú, 1982. ISBN: 950-14-0020-4.

CASABIANCA ZULETA, Paola. *Las intervenciones telefónicas en el sistema penal.* Barcelona: Bosch, 2016. ISBN: 978-84-944790-0-7.

CRUZ RIVERO, Diego. La suplantación de identidad en el ámbito electrónico y la defraudación de la banca electrónica. *Revista de derecho bancario y bursátil.* 2010, Nº 117, págs. 191-230. ISSN: 0211-6138.

DE LA MATA BARRANCO, Norberto J., HERNÁNDEZ DÍAZ, Leyre. Los delitos vinculados a la informática en el Derecho Penal español. En: DE LA CUESTA ARZAMENDI, José Luís. *Derecho penal informático.* Madrid: Civitas, 2010. ISBN: 978-84-470-3429-1. Págs.: 159-200.

DE LA MATA BARRANCO, Norberto J., HERNÁNDEZ DÍAZ, Leyre. Un ejemplo de delitos informáticos: Delitos contra sistemas y datos en el Código Penal español ¿delitos de daños? En: DE LA CUESTA ARZAMENDI, José Luís. *Derecho penal informático.* Madrid: Civitas, 2010. ISBN: 978-84-470-3429-1. Págs.: 201-246.

DE LAS HERAS MUÑOS, Mar. Medios de prueba. Informática forense y peritaje informático. En: BUENO DE MATA, Federico. *Fodertics: estudios sobre derecho y nuevas tecnologías.* Santiago de Compostela: Andavira, D.L.2012. ISBN: 978-84-8408-692-5.

DOMINGUEZ MATEOS, Isabel. ESTEBAN RUIZ, Adaya María. GARCÍA DE PABLOS, María. Sextorsión: Tortura en la Red. En: BUENO DE MATA, Federico. *Fodertics 4.0: (estudios sobre nuevas tecnologías y justicia).* Granada: Comares, 2015. Págs.: 155-162. ISBN: 978-84-9045-274-5. Pág.:156.

FERNANDEZ TERUELO, Javier Gustavo. *Derecho penal e internet: especial consideración de los delitos que afectan a jóvenes y adolescente.* Valladolid: Lex Nova, 2011. ISBN: 978-84-9898-365-4.

GUDÍN RODRIGUEZ-MAGARIÑOS, Faustino. Algunas consideraciones sobre el nuevo delito de Grooming. En: *Delincuencia informática. Tiempos de cautela y amparo.* Cizur Menor (Navarra): Thomson Reuters Aranzadi, 2012. Págs.: 141-149. ISBN: 978-84-9014-273-8.

GUDÍN RODIGUEZ-MAGARIÑOS, Faustino. La lucha contra el ciberblanqueo como vía para acabar con el pishing. *Revista Aranzadi Doctrinal.* 2014, Nº. Extra 9-10, págs. 261-293. ISSN: 1889-4380.

ILLÁN FERNÁNDEZ, José María. *La prueba electrónica, eficacia y valoración en el proceso civil.* Cizur Menor (Navarra): Aranzadi, 2009. ISBN: 978-84-9903-396-9.

LORENTE LÓPEZ, María Cristina. La vulneración de los derechos al honor, a la intimidad y a la propia imagen de los menores a través de las Nuevas Tecnologías. *Revista Aranzadi Doctrinal.* 2015, Nº 2, págs..: 201-222. ISSN: 1889-4380.

MEDINA LINÀS, Manel. *Cibercrimen: ¡protégete del "bit-bang"!, los ataques en el ciberespacio a tu ordenador, tu móvil, tu empresa: aprende de víctimas, expertos y cibervigilantes.* Barcelona: Tibidabo, 2015. ISBN: 978-84-16204-82-3.

MUERZA ESPARZA, Julio. La reforma procesal penal de 2015. *Aranzadi digital parte Estudios y comentarios.* 2015, Nº 1 (BIB 2015\16990).

ORTIZ PRADILLO, Juan Carlos. Hacking legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática. En: *Delincuencia informática. Tiempos de cautela y amparo.* Cizur Menor (Navarra): Thomson Reuters Aranzadi, 2012. Págs.: 177-220. ISBN: 978-84-9014-273-8. Pág.: 194.

REZENDE CECILIO, Leonardo. Política criminal en el ciberespacio: critica al concepto de crimen informático. En: BUENO DE MATA, Federico. *Fodertics 3.0: (estudios sobre nuevas tecnologías y justicia).* Granada: Comares, 2015. ISBN: 978-84-9045-239-4.

REYES LÓPEZ, Javier Ignacio. Los dispositivos técnicos de geolocalización. Régimen jurídico a partir de la LO 13/2015. *Revista Aranzadi Doctrinal.* 2016, Nº 9. Págs.: 53-66. ISSN: 1889-4380.

URBANO CASTRILLO, Eduardo, MAGRO SERVET, Vicente. *La prueba tecnológica en la Ley de Enjuiciamiento Civil.* Cizur Menor (Navarra): Aranzadi, 2003. ISBN: 847671015.

URBANO CASTRILLO, Eduardo. *La valoración de la prueba electrónica.* Valencia: Tirant lo Blanch, 2009. ISBN: 978-84-9876-445-1.

VELASCO SAN MARTÍN, Cristos. *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet.* Valencia: Tirant lo Blanch, 2012. ISBN: 978-84-9004-981-5.

VIDAL MARÍN, Tomás. RUIZ DORADO, María. Análisis de la constitucionalidad del SITEL. Breves consideraciones a partir de la Ley Orgánica 13/2015, de reforma de

la Ley de Enjuiciamiento Criminal. *Revista Aranzadi Doctrinal.* 2016, Nº 9. ISSN:1889-4380.

VILLACAMPA ESTIARTE, Carolina. *El delito de "online child grooming" o propuesta sexual telemática a menores.* Valencia: Tirant lo Blanch, 2015. ISBN: 978-84-9086-445-6.

ASENCIO MELLADO, José María. *La prueba documental. Concepto y regulación legal.* (http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUsDC1NDtbLUouLM_DxbIwNDY0MjQ0uQQGZapUt-ckhlQaptWmJOcSoA4ZERPTUAAAA=WKE) [Fecha de consulta: 30-08-2016].

Autor desconocido. *Calificación jurídica del mulero en el phising.* (http://es.slideshare.net/rafameca/calificacin-jurdica-del-mulero-en-el-phising). [Fecha de consulta:11-10-2016].

BENTHAM, M. Jeremías. *Tratado de las Pruebas Judiciales.* París: Bossange Frerres, 1825. Tomo Primero. Pág.: 19. (http://cdigital.dgb.uanl.mx/la/1080045433_C/1080045433_T1/1080045433_MA.PDF).

CNUDMI. *Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005).* (http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2005Convention.html) [Fecha de consulta: 31-08-2016].

DUARTE, Eugenio. *7 tipos de hackers y sus motivaciones.* (http://blog.capacityacademy.com/2012/07/11/7-tipos-de-hackers-y-sus-motivaciones/). [Fecha de consulta: 07-10-2016].

EFE. *Tres años y medio de cárcel por amputarse una mano para estafar al seguro*. (http://www.rtve.es/noticias/20161014/tres-anos-medio-carcel-amputarse-mano-para-estafar-seguro/1425783.shtml). [Fecha de consulta: 20-11-2016].

FLORES FERNÁNDES, Jorge. *Sexting: adolescentes, sexo y teléfonos móviles.* (http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/pdfs/pantallasamigas-sexting-adolescentes-sexo-y-telefonos-moviles.pdf). [Fecha de consulta: 13-10-2016].

FLORES FERNÁNDEZ, Jorge. *Ciberbullying. Guía rápida.* (http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/pdfs/pantallasamigas-ciberbullying-guia-rapida.pdf). [Fecha de consulta: 14-10-2016].

GÓMEZ DEL CASTILLO Y GÓMEZ, Manuel M. *Aproximación a los nuevos medios de prueba en el proceso civil.* (http://rabida.uhu.es/dspace/bitstream/handle/10272/1546/b1205663.pdf?sequence=1) [Fecha de consulta: 28-08-2016].

GONZÁLEZ, Daniel. *Tecnologías de la Información y la Comunicación.* (http://www.monografias.com/trabajos67/tics/tics.shtml#ixzz4IuE8WAzB) [Fecha de consulta: 28-08-2016].

GUARDIOLA SALMERÓN, Miriam. *El "sexteo", el "sexting" y la "sextorsión".* (http://www.lawandtrends.com/noticias/penal/el-sexteo-el-sexting-y-la-sextorsion.html). [Fecha de consulta: 13-10-2016].

GUDÍN RODRIGUEZ-MAGARIÑOS, Fausto. *Nuevos delitos informáticos: phising, pharming, hacking y cracking.* (http://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20informáticos.pdf) [Fecha de consulta: 10-10-2016].

INSA MÉRIDA, Fredesvinda, LÁZARO HERRERO, Carmen, GARCÍA GÓNZALEZ, Nuria. *Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad. Un proyecto europeo.* (http://www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1690-75152008000200009). [Fecha de consulta: 28-08-2016].

INSA MÉRIDA, Fredesvinda. *El Certificado Europeo sobre Cibercriminalidad y Prueba Electrónica (ECCE): Un gran proyecto de formación para los profesionales del mundo jurídico.* (http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUMzSwNLtbLUouLM_DxbIwMDSwMjIzOQQGZapUt-ckhlQaptWmJOcSoA-tOpMTUAAAA=WKE). [Fecha de consulta: 31-08-2016].

LÓPEZ AZAMAR, Bertha. *Software malintencionado e infeccioso.* (http://www.unpa.edu.mx/~blopez/Computacion/complementario/VirusYotrosMalware.pdf). [Fecha de consulta: 12-10-2016].

MADARIAGA, Bárbara. *Llega la primera Certificación Europea sobre Cibercriminalidad y Pruebas Electrónicas.* (http://www.dealerworld.es/seguridad/llega-la-primera-certificacion-europea-sobre-cibercriminalidad-y-pruebas-electronicas). [Fecha de consulta: 31-08-2016].

MALENKOVICH, Serge. *7 pasos para recuperarnos del Scareware.* (https://blog.kaspersky.es/7-pasos-para-recuperarnos-del-scareware/165/). Fecha de consulta: 12-10-2016].

MARTI, Miriam. *Las Siete Partidas, leyes de la antigua Castilla.* (http://historiageneral.com/2013/01/17/las-siete-partidas-leyes-de-la-antigua-castilla/) [Fecha de consulta: 28-08-2016].

MATELLANES RODÍGUEZ, Nuria. *Vías para la tipificación del acceso ilegal a los sistemas*.

(http://www.uhu.es/revistapenal/index.php/penal/article/viewFile/362/353). [Fecha de consulta: 07-10-2016].

OXMAN VILCHES, Nicolás André. *Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"*. (http://www.scielo.cl/pdf/rdpucv/n41/a07.pdf). [Fecha de consulta: 12-10-2016].

PALMA, Antonio. *Cómo conocer el código IMEI de mi móvil.* (http://tecnologia.uncomo.com/articulo/como-conocer-el-codigo-imei-de-mi-movil-18353.html). [Fecha de consulta: 20-10-2016].

PÉREZ PALACÍ, José Enrique. *La prueba electrónica: Consideraciones.* (http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39084/1/PruebaElectronica 2014.pdf) [Fecha de consulta: 31-08-2016].

REDACCIÓN NJ. *El 89,5% de los expertos jurídicos europeos equipara la validez de la prueba electrónica con la tradicional.* (http://noticias.juridicas.com/actualidad/noticias/26-el-89-5-de-los-expertos-juridicos-europeos-equipara-la-validez-de-la-prueba-electronica-con-la-tradicional/) [Fecha de consulta: 31-08-2016].

REDACCIÓN NJ. *La grabación realizada en la vía pública y por detectives de la aseguradora, de la víctima de un accidente de tráfico, no vulnera su derecho a la vida privada.* (http://noticias.juridicas.com/actualidad/noticias/3817-la-grabacion-realizada-en-la-via-publica-y-por-detectives-de-la-aseguradora-de-la-victima-de-un-accidente-de-trafico-no-vulnera-su-derecho-a-la-vida-privada/). [Fecha de consulta: 20-11-2016].

REY HUIDOBRO, Luis Fernando. *La estafa informática: relevancia penal del phising y el pharming.* (http://www.bufetelineros.eu/es/noticia.asp?pag=&id=2491&por=1) [Fecha de consulta: 12-10-2016].

RODRIGUEZ CARO, María Victoria. Estafa informática. *El denominado phishing y la conducta del "mulero bancario": categorización y doctrina de la Sala Segunda del Tribunal Supremo.* (http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo%3Bmulero/) [Fecha de consulta:12-10-2016].

Rubén Andrés. *Cómo saber cuál es la dirección IP de mi ordenador*. (http://computerhoy.com/paso-a-paso/internet/como-saber-cual-es-direccion-ip-mi-ordenador-24347). [Fecha de consulta: 20-10-2016].

RUIZ SERRA, Joana. *Artículo 26 del código penal: el documento (España)* (http://www.monografias.com/trabajos104/articulo-26-del-codigo-penal-documento/articulo-26-del-codigo-penal-documento.shtml#ixzz4KG2zNNuB) [Fecha de consulta: 13-09-2016].

SAN MIGUEL, Axel. *8 tipos de hackers que debes conocer.* (http://axelsanmiguel.com/8-tipos-de-hackers-que-debes-conocer/). [Fecha de consulta: 07-10-2016].

SAPENE CISNEROS, Juan Enrique. *Phishing ¿Qué es? ¿Cómo lo hacen? ¿Cómo evitarlo?* (https://www.digitalconexion.com/newsite/Phishing-Que-es-Como-lo-hacen-Como-evitarlo.html). [Fecha de consulta: 11-10-2016].

TABUENCA, Alex. *El cortafuegos: phishing y pharming.* (http://elcortafuegosdeinternet.blogspot.com.es/2010/06/phising-y-pharming.html). [Fecha de consulta: 12-10-2016]

TENZER, Simón Mario. *Riesgo Informático: "Spyware", "Adware" y "Popup".* (http://www.ccee.edu.uy/ensenian/catcomp/material/Inform_%20II/SPYWARE.PDF). [Fecha de consulta: 12-10-2016].

TORRES, Mònica. *La policía quiere que los niños sean Ciberexpert@s.* (http://elpais.com/elpais/2016/06/02/actualidad/1464875428_167957.html). [Fecha de consulta: 14-10-16].

URIARTE VALIENTE, Luis M. *Nuevas técnicas de investigación restrictivas de derechos fundamentales.* (https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Sr%20Uriarte%20Valiente.pdf?idFile=ec583d09-edd5-4a96-b303-a9fca37cf99e). [Fecha de consulta: 20-11-2016].

VELASCO NÚÑEZ, Eloy. *Los delitos informáticos: la reparación y las indemnizaciones. Especial referencia al fraude.* (http://www.elderecho.com/tribuna/penal/informaticos-reparacion-indemnizaciones-Especial-referencia_11_194680019.html). [Fecha de consulta: 11-10-2016].

VELASCO SAN MARTÍN, Cristos, JIMÉNEZ ROJAS, Jesús Ramón. *Spyware, el software espía.* (http://www.enterate.unam.mx/Articulos/2005/marzo/spyware.htm). [Fecha de consulta: 12-10-2016].

VICENTE DE ANTONIO, Javier. *La moda de los drones arrasa en Salamanca.* (http://www.salamanca24horas.com/local/13-10-2016-alarmante-aumento-de-adicciones-y-ciberacoso-adolescentes-por-internet). [Fecha de consulta: 20-11-2

ANEXO JURISPRUDENCIAL

- **Sentencias del Tribunal Europeo de Derechos Humanos**

1. STEDH 1 marzo 2001 (TEDH 2011/26)
2. STEDH 27 mayo 2014 (TEDH 2014/34)

- **Sentencias del Tribunal Constitucional**

1. STco. 6 junio 1995 (RTC 1995/86)
2. STco. 26 marzo 1996 (RTC 1996/49)
3. STco. 26 marzo 1996 (RTC 1996/54)
4. STco. 17 septiembre 1999 (RTC 1999/219)
5. STco. 14 febrero 2005 (RTC 2005/25)
6. STco. 3 abril 2006 (RTC 2006/104)
7. STco. 27 abril 2010 (RTC 2010/26)
8. STco. 9 mayo 2013 (RTC 2013/115)
9. STco. 22 septiembre 2014 (RTC 2014/145)

- **Sentencias del Tribunal Supremo**

1. STS 1 marzo 1996 (RJ 1996/1886)
2. STS 10 febrero 1998 (RJ 1998\948)
3. STS 26 febrero 1998 (RTC 1998/1467)
4. STS 15 febrero 1999 (RJ 1999/1918)
5. STS 20 noviembre 2001 (RJ 2002\805)
6. STS 1 abril 2002 (RJ 2002/5444)
7. STS 12 junio 2002 (RJ 2002/8419)
8. STS 14 octubre 2002 (RJ 2002\8963)
9. STS 7 marzo 2003 (RJ 2003/2815)
10. STS 13 marzo 2003 (RJ 2003/2662)

11. STS 23 enero 2007 (RJ 2007/2316)

12. STS 19 febrero 2007 (RJ 2007/1809)

13. STS 22 junio 2007 (RJ 2007/5318)

14. STS 3 octubre 2007 (RJ 2007/6289)

15. STS 3 octubre 2007 (RJ 2007/7297)

16. STS 9 mayo 2008 (RJ 2008/4648)

17. STS 20 mayo 2008 (RJ 2008/4387)

18. STS 11 junio 2008 (RJ 2008/4655)

19. STS 18 junio 2008 (RJ 2008/3664)

20. STS 12 noviembre 2008 (RJ 2009/167)

21. STS 6 febrero 2009 (RJ 2009/3065)

22. STS 6 julio 2009 (RJ 2009/5977)

23. STS 28 septiembre 2009 (RTC 2009/197)

24. TS, auto de 12 noviembre 2009 (JUR 2009/474656)

25. STS 19 noviembre 2009 (RJ 2009/7906)

26. STS 31 marzo 2010 (RJ 2010/5547)

27. STS 25 abril 2010 (RJ 2010/4922)

28. STS 19 mayo 2010 (RJ 2010/5821)

29. STS 2 junio 2010 (RJ 2010/3489)

30. STS 14 julio 2010 (RJ 2010/3509)

31. STS 29 diciembre 2010 (RJ 2011/135)

32. STS 15 marzo 2011 (RJ 2011/2783)

33. STS 7 abril 2011 (RJ 2011/3341)

34. STS 10 mayo 2011 (RJ 2011/5731)

35. STS 26 mayo 2011 (RJ 2011/4049)

36. STS 24 junio 2011 (RJ 2011/5133)
37. STS 7 noviembre 2011 (RTC 2011/173)
38. STS 17 noviembre 2011 (RJ 2012/11372)
39. STS 6 julio 2012 (RJ 2012/9445)
40. STS 17 abril 2013 (RJ 2013/3296)
41. STS 18 abril 2013 (RJ 2013/8007)
42. STS 14 mayo 2013 (RJ 2013/3727)
43. STS 28 junio 2013 (RJ 2013/8067)
44. STS 5 noviembre 2013 (RJ 2013/7729)
45. STS 6 noviembre 2013 (RJ 2013/7467)
46. STS 7 noviembre 2013 (RJ 2013/7468)
47. STS 26 diciembre 2013 (RJ 2014/420)
48. STS 16 mayo 2014 (RJ 2014/2937)
49. STS 9 junio 2014 (RJ 2014\3398)
50. STS 15 julio 2016 (RJ 2016/3758)

❖ **Sentencias de la Audiencia Nacional**

1. SAN 26 julio 2008 (JUR 2008/246898)
2. SAN 13 abril 2015 (JUR 2015/135793)

❖ **Sentencias de la Audiencia Provincial**

1. SAP Barcelona (Sección 13ª) 2 de mayo 2007 (JUR 2007/270189)
2. SAP Lleida (Sección 1ª) 19 junio 2014 (ARP 2014\1006)
3. SAP Madrid 23 octubre 2015 (ARP 2015/1261)

❖ **Sentencias de Tribunales Superiores de Justicia**

1. STSJ Madrid 6 de julio (AS 2004/2325)
2. STSJ Andalucía 28 de enero, Málaga (AS 2000/146)

3. STSJ Andalucía 12 junio 2013, Granada (ARP 2013/707)
4. STSJ Cataluña 10 abril 2014 (ARP 2014/774)
5. STSJ Cataluña 23 julio 2015 (JUR 2015/241338)

❖ **<u>Sentencias de Juzgados de lo Penal</u>**

1. SJP Nº3 Gijón 6 julio 2016 (ARP 2016/843),