UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO INTERNACIONAL PÚBLICO

TESIS DOCTORAL

DATOS DE GEOLOCALIZACIÓN COMO MEDIDA DE INVESTIGACIÓN. AVANCES EN EL SISTEMA JURÍDICO PROCESAL PENAL

LAURA MARÍA CABELLO GIL

LICENCIADA EN DERECHO

Director de la tesis: Dr. D. FERNANDO MOURE COLÓN

Centro Universitario de la Guardia Civil

Tutor: Dra. Dª. FANNY CASTRO-RIAL GARRONE

2017

UNED
DEPARTAMENTO DE DERECHO INTERNACIONAL PÚBLICO
Facultad de Derecho

DATOS DE GEOLOCALIZACIÓN COMO MEDIDA DE INVESTIGACIÓN. AVANCES EN EL SISTEMA JURÍDICO PROCESAL PENAL

LAURA MARÍA CABELLO GIL
Licenciada en Derecho

Director de la tesis: Dr. D. FERNANDO MOURE COLÓN

Tutor: Dra. Dª. FANNY CASTRO-RIAL GARRONE

A mi familia,
a mi marido Ignacio por confiar en mí,
a mis hijos Oscar y Nacho,
por los momentos que les he robado de estar con ellos
y a mi ángel, por iluminarme todos los días.

A mi madre, por todo.
A mi padre, por ser ejemplo de trabajo.

A Ignacio, por todos sus puntos y comas. Gracias.

A mi director de tesis Dr. D. Fernando Moure,
por hacer fácil lo imposible.

A los que me habéis apoyado en esta última etapa.
Sin vosotros, esta tesis no habría visto la luz.

Muchas gracias.

ÍNDICE

TABLA DE ILUSTRACIONES

ABREVIATURAS

A-GPS	*Assisted-Global Positioning System*
AEPD	Agencia Española de Protección de Datos
art./arts.	Artículo/artículos
BOE	Boletín Oficial del Estado
BTS	*Base Transceiver Station*
CDR	*Call Data Record*
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
Coord.	Coordinador
CS	Estaciones de control
DNS	*Domain Name Server*
DOUE	Diario Oficial de la Unión Europea
Dtor.	Director
ed.	Edición
etc.	Etcétera
Exif	*Exchangeable Image File Format*
FJ	Fundamento Jurídico
FS	Estaciones fijas

GMDSS	*Global Maritime Distress Safety System*
GPS	*Global Positioning System*
GSM	*Global System for Mobile*
HLR	*Home Location Register*
ICANN	*Internet Corporation for Asigned Names and Numbers*
IMEI	*International Mobile Equipment Identity*
IMSI	*International Mobile Subscriber Identity*
IO	Internet de los Objetos
IP	*Internet Protocol*
IM	Mensajería instantánea
km	Kilómetro
L	Ley
LAI	*Location Area Identifier*
LBS	*Location Based Services*
LCDCE	Ley 25/2007, de 18 de octubre de conservación de datos relativas a las comunicaciones electrónicas y a las redes públicas de comunicaciones
LECrim	Ley de Enjuiciamiento Criminal
LGT	Ley General de Telecomunicaciones
LO	Ley Orgánica
LOPDCP	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LOPJ	Ley Orgánica del Poder Judicial
LTE	*Long Term Evolution*

LSSICE	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
MAC	*Medium Access Control*
MMS	*Multimedia Messaging Service*
MS	Estaciones móviles
NGN	*Next Generation Working*
núm.	Número
p.	Página
p.e.	Por ejemplo
P2P	*Peer to Peer*
PSI	Proveedores de servicios de Internet
RAE	Real Academia Española
RD	Real Decreto
RDL	Real Decreto Ley
rec.	Recurso
RPDCP	Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
RS	Estaciones repetidoras
SIM	*Subscriber Identity Module*
SMS	*Short Message Service*
SSID	*Service Set Identifier*
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STS	Sentencia del Tribunal Supremo

STC	Sentencia del Tribunal Constitucional
TC	Tribunal Constitucional
TDOA	*Time Difference of Arrival*
TEDH	Tribunal Europeo de Derechos Humanos
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones
vs.	*Versus*
VHF	*Very High Frequency*
VoIP	*Voice over IP*
Vol.	Volumen
VRL	*Visitor Location Register*
VV.AA.	Varios autores
WAP	*Wireless Application Protocol*
WEP	*Wired Equivalent Privacy*
WLAN	*Wireless LAN*
WPA	*WiFi Protected Access*

INTRODUCCIÓN

El avance de las nuevas tecnologías en nuestra sociedad es incuestionable, y la superación de la norma y la jurisprudencia por la realidad moderna es un hecho, dejándolas cada vez más obsoletas.

De una parte, la expansión de las redes de telecomunicaciones supone un importante desafío para la sociedad actual, en el sentido de encontrarnos ante procesos comunicativos en el entorno informático cada vez más complejos y sofisticados, que han superado con creces a la norma, y que necesitan de una protección jurídica actualizada ante las más que posibles amenazas emergentes en la conocida como sociedad de la información del siglo XXI. Contamos con sistemas GPS como dispositivos autónomos y como parte integrante de nuestro dispositivo de comunicación móvil, redes *WiFi* que transmiten información de nuestra localización más allá de la que el ciudadano voluntariamente desea, archivos *Exif* en nuestras fotos que integran datos de la ubicación, estaciones base de telefonía que recogen de manera constante nuestra situación espacial... múltiples variantes que merecen ser analizadas ante la laguna jurídica existente.

Vemos como nuestra sociedad actual es cada vez más dinámica y cambiante, y este hecho implica necesariamente la profundización en el análisis de los problemas jurídicos surgentes, con el objeto de adecuar el ordenamiento jurídico a las consiguientes transformaciones técnicas y sociales.

Este estudio se configura como investigación jurídica teórico-práctica, puesto que, en cuanto actividad intelectual, tiene como objetivo encontrar las soluciones jurídicas adecuadas a los problemas que plantea socialmente la evolución, el uso y la aplicación de las nuevas tecnologías a la geolocalización de las personas.

El alcance de la investigación no solo se limita a realizar un estudio bibliográfico, y por tanto cualitativo, de recopilación de información y consulta, tanto de fuentes accesibles al público general, como de textos ya existentes sobre la materia. En este ámbito cualitativo, destacar que se pretende realizar un extenso análisis documental, que se complementa con la experiencia profesional de campo desarrollada por parte de la autora. Destacando, como instrumentos y técnicas de recolección de datos en este ámbito, la obtención de los disponibles en normas legales y reglamentarias, manuales editados por las autoridades competentes, bases de datos jurídicas y consulta en bibliotecas y sitios web especializados que vienen debidamente referenciados en la bibliografía de esta tesis doctoral.

Se valora el hecho del desarrollo de la técnica y de las comunicaciones desde un punto de vista objetivo, determinando qué instrumentos, existentes en la actualidad, nos sirven para informar de la ubicación de una persona, con la consiguiente utilidad que ello reporta a la investigación de los ilícitos penales por las unidades policiales. A este hecho, se le vincula un posicionamiento doctrinal al respecto, una jurisprudencia avanzada con respecto a la norma, y por fin, aunque de modo incompleto, una legislación relacionada con esta materia que requiere de interpretación, la cual busca como objetivo rellenar el patente vacío legal.

Más concretamente, el planteamiento inicial se basa en un estudio objetivo y real, dentro del Capítulo I, de la situación de facto de los datos de geolocalización, especificando no solo su tipología desde el punto de vista de la técnica, sino el abanico de normas existentes al respecto.

Tras ello, usando un tipo de saber reflexivo, y tras estar en posesión consciente de la realidad geolocativa, se emiten, en el Capítulo II, juicios explicativos, comprensivos y demostrables, que traen fundamento de la doctrina y la jurisprudencia, sin olvidarnos de la interpretación de la escasa norma, en relación con la obtención y/o intervención de los datos de localización dentro del marco de una investigación penal.

Posteriormente, y ya en el Capítulo III, se presenta la utilidad procesal de dichos datos; usando un método deductivo se alcanzan conclusiones en relación al posible peso probatorio en el proceso penal de esta nueva información lograda tras un proceso de desarrollo de la tecnología.

Así pues, se puede afirmar que la presente investigación engloba todo un conjunto de procedimientos de carácter reflexivo, sistemático, controlado, crítico y creativo cuyo objetivo es la búsqueda, la indagación, el estudio, y la aplicación de las norma, hechos y valores que, considerando la dinámica de los cambios sociales, políticos, económicos y culturales actuales, afectan al campo de la geolocalización y de la comunicación subsiguiente, sin rebasar los límites jurídicos de confidencialidad e intimidad de la persona, así como los impuestos por el derecho al secreto de las comunicaciones.

Las soluciones que se aportan en la tesis pueden someterse a prueba, verificando su coherencia, sus fundamentos legales y su concreción específica, pues el individuo y su geolocalización exigen investigación de lo concreto, de los diversos supuestos que se dan en la realidad y alejarnos de generalidades, las cuales no son adecuadas a tenor de la pluridimensionalidad de la información geolocativa.

Se logrará con ello tener una visión clara y completa de los datos de geolocalización, de su tipología, de su naturaleza jurídica, la legislación

aplicable a cada supuesto y su modo de introducción en el proceso penal, dejando atrás el entramado complejo y confuso que conforman las escasas disposiciones expresas que regulan esta materia, y la dispersa jurisprudencia dictada a la luz de casos concretos.

Los datos de geolocalización como hecho dejarán de ser desconocidos y, como concepto jurídico, encontrarán su ubicación en las distintas y diseminadas normas, dependiendo siempre de su variable naturaleza jurídica. Se le reconocerá su innegable peso como medida de investigación, fuente de prueba y en su caso, medio de prueba, quedando delimitados los márgenes legales entre los que se desarrolla esta información sobre la ubicación de las personas.

CAPÍTULO I

DATOS DE GEOLOCALIZACIÓN

Los dispositivos que permiten ubicar geográficamente los objetos y a las personas que los portan, junto con la elaboración de los perfiles de sus movimientos, constituyen hoy por hoy elementos indispensables en muchas investigaciones penales. Su utilidad probatoria es además incuestionable en la medida en que pueden ser hábiles para acreditar de manera fidedigna que algo se hallaba o pasó por un lugar en un momento preciso, que siguió una determinada trayectoria, la frecuencia con la que concurría en un mismo ámbito espacial, los sujetos que coincidían en el tiempo en un mismo lugar, etc. En virtud del más que aceptable grado de precisión que la técnica posibilita, constituyen indicios muy poderosos que, debidamente ligados entre sí y con otros, vincularán a personas con hechos concretos en aras de formar la convicción judicial sobre la participación de aquellas en estos[1].

[1] PÉREZ GIL, J., *Los datos sobre localización geográfica en la investigación penal*, en "Protección de datos y proceso penal", 1ª edición, Editorial LA LEY, Madrid, junio 2010.

Más concretamente, los *smartphones* o *tablets* están estrechamente vinculados a su usuario, de modo que rara vez este se separa de su dispositivo móvil o se lo presta a otra persona. Como podremos ver, estos dispositivos móviles contienen una gran información personal de su usuario, desde *emails* a fotografías, contactos etc., lo que permite a los proveedores de servicios disponer de una panorámica detallada de los hábitos y pautas del propietario del terminal, pudiendo elaborar un perfil del mismo o modelo de comportamiento (por ejemplo, se podrían conocer sus visitas a lugares de culto, horarios de trabajo, presencia en actos políticos, amistades…).

Así, entre los grandes riesgos a los que se enfrentan los propietarios, se encuentra que estos no se percaten de que están transmitiendo su localización y mucho menos a quién, o, por ejemplo, que el consentimiento para determinadas aplicaciones que utilizan sus datos de localización no sea válido, debido a que la información sobre los elementos clave del procesamiento sea incomprensible, anticuada o insuficiente por cualquier otro motivo, como veremos posteriormente.

Ya en el marco de la investigación de un sospechoso, la tecnovigilancia se ha convertido en algo frecuente. La injerencia no física en espacios propios de la privacidad del sospechoso, mediante las nuevas herramientas tecnológicas, amplían las posibilidades de obtención de información, con total reserva y sigilo, superando con mucho la que

tradicionalmente se lograba a través de lo que el investigador podía percibir con sus sentidos.

Esta nueva tecnología no solo varía la forma de delinquir y de investigar al delincuente, sino que modifica las expectativas de privacidad de la población en general, y más concretamente del derecho del ciudadano a no estar localizado de manera continua y de forma ilimitada.

Hemos de partir de la idea de la deficiente regulación al respecto, y ello no porque no exista, sino porque está diseminada en múltiples textos legislativos relacionados con solo algunos tipos de datos de geolocalización.

Como se expondrá en este capítulo, son múltiples las variantes que la técnica pone a nuestra disposición para averiguar la ubicación de una persona, y no todas ellas están recogidas por la norma. Se hace necesario conocer en primer lugar, desde un punto de vista tecnológico y sin ánimo de ser exhaustivo, la tipología básica de los datos de geolocalización para posteriormente identificar qué regulación jurídica existe en relación con dicha materia. De este contraste de datos, podremos obtener, como resultado, una visión clara del ámbito jurídico actual y vigente de los datos de geolocalización.

I.- IDENTIFICACIÓN Y CLASES DE DATOS DE GEOLOCALIZACIÓN

Los sistemas electrónicos de posicionamiento global esconden realmente diversas herramientas de trabajo que utilizan principalmente, bien las señales facilitadas por los satélites que conforman el sistema GPS[2], bien la interactuación de estaciones BTS o redes *WiFi*[3]. Tal interactuación de señales que circulan tanto por el espectro radioeléctrico, como a través de las redes GSM[4] hace que los derechos fundamentales en conflicto, cuando de una injerencia sobre la información almacenada en aquellos se trata, puedan bascular entre la protección formal del artículo 18.3 de la Constitución Española y la salvaguardia de la intimidad y otros datos de carácter personal o artículo 18.1 en relación con el 18.4 de la norma suprema, con las consecuencias que podrían derivarse de tal diferencia[5].

[2] La tecnología GPS (sistema de posicionamiento global por satélite o *Global Positioning System*) utiliza 31 satélites que giran en 6 órbitas diferentes alrededor de la Tierra; cada satélite transmite una señal radioeléctrica muy precisa. El dispositivo móvil puede determinar su ubicación, cuando la antena del GPS recibe al menos 4 de dichas señales. Esta señal es diferente de los datos de las estaciones de base porque solo viaja en un sentido. Las entidades que gestionan los satélites no tienen capacidad para establecer un registro de los dispositivos que han recibido la señal radioeléctrica. La tecnología GPS ofrece un posicionamiento exacto, de entre 4 y 15 metros.

Vid., UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 DE LA DIRECTIVA 95/46/CE, Dictamen 13/2011, de 16 de mayo de 2011, sobre los servicios de geolocalización en dispositivos móviles inteligentes, p.5.

[3] *WiFi* o mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

[4] GSM o *Global System for Mobile*. Sistema empleado por las antenas para las comunicaciones móviles.

[5] RODRÍGUEZ LAÍNZ, J.L., *Los dispositivos electrónicos de posicionamiento global (GPS) en el Proceso Penal*, Diario La Ley, núm. 7945, Sección Doctrina, Ref. D-358, Editorial LA LEY, 17 octubre de 2012.

I.1.-Sistema GPS en móvil y como dispositivo autónomo

Los conocidos dispositivos receptores GPS se han visto mejorados en un breve lapso de tiempo por una tecnología híbrida tendente a reducir al máximo posible las disfunciones de funcionamiento, consecuencia de la existencia de zonas de baja cobertura, o los problemas derivados de la detección de satélites al activar el dispositivo. Así, nos encontramos con los dispositivos A-GPS[6], auxiliados por servidores de asistencia modo *on line*, que facilitarían, vía red de comunicaciones electrónicas, información adicional o tendente a proveer una mejora de calidad y rapidez del sistema.

La tecnología GPS ofrece un posicionamiento exacto, de entre 4 y 15 metros, convirtiéndose ello en su mayor ventaja frente a inconvenientes: arranque o detección inicial de la señal GPS relativamente lentos, o mal funcionamiento en lugares cerrados, por ejemplo.

Frente al sistema anterior de posicionamiento global basado en satélites lanzados por Estados Unidos para inicialmente fines militares, la Comisión Europea ideó el Programa Galileo, diseñado para comenzar a funcionar en el 2014, y consistente en una red de 18 satélites, situados en órbita media, que va a ofrecer un sistema mundial de radionavegación

[6] A-GPS o *Assisted-Global Positioning System.*

por satélite gratuito y de uso civil[7], que se prevé estará plenamente operativo en el 2020.

Este sistema consta de cuatro componentes principales[8]:

- *Elemento Global*, que proporcionará los servicios básicos a nivel global y estará compuesto por una constelación de satélites (treinta) encargados de proporcionar la señal de navegación, siendo controlados por centros de control o estaciones de enlace civiles que vigilan la señal enviada por los satélites y determina las órbitas de estos con alta precisión.

- *Elemento Regional*, que conseguirá mayores prestaciones sobre una región determinada; el número máximo de regiones a cubrir es de seis.

- *Elemento Local*, que incrementará la integridad y la precisión sobre áreas locales, recurriendo a estaciones situadas en puntos conocidos con una alta precisión; podrá calcular errores existentes en la señal Galileo y difundirlos a los usuarios a través de un

[7] COMISIÓN EUROPEA. Programa Galileo. Recuperado de: http://cordis.europa.eu/programme/rcn/871_es.html (última consulta: 2 de noviembre de 2016).

[8] ANDRADA MÁRQUEZ, L., *Galileo: El sistema europeo de navegación por satélite*, División de Navegación por Satélite. Aeropuertos Españoles y Navegación Aérea (AENA). Recuperado de: https://www.coit.es/archivo-bit/mayo-junio-2001/telecomunicaciones-y-navegacion-por-satelite-galileo-el-sistema-europeo (última consulta: 3 de marzo de 2015).

medio de comunicación de corto alcance (por ejemplo VHF), permitiendo un alcance de 50 km.

- *Elemento Usuario*, encargado de extraer la información contenida en las señales enviadas por los satélites y de presentarla al usuario en forma comprensible, siendo sus receptores desarrollados para diferentes tipos de destinatarios y en función de las necesidades del mercado de las aplicaciones.

En cuanto a los servicios que va a ofrecer, se cuenta con:

- *Servicio abierto*, el cual proporcionará señales de navegación, posicionamiento y tiempo a las que se podrá acceder de forma gratuita, de modo similar al GPS. Este servicio, por tanto, será accesible al mercado de la población en general, dentro de las aplicaciones de navegación, tales como navegadores de coche o *smartphones*, *tablets* etc.

- *Servicio comercial*, que proporcionará un valor añadido con respecto al anterior, al disponer de prestaciones mejoradas basadas en el diseño de la señal. Las prestaciones concretas de este servicio podrán ser definidas por los proveedores de servicio teniendo en cuenta la calidad de los datos comerciales difundidos y las prestaciones conseguidas por los componentes locales.

- Servicio *Safety of Life*, cuyas prestaciones han sido concebidas no solo para cubrir las necesidades aeronáuticas, sino las de otros modos de transporte, pudiendo ser usado como medio único de navegación al disponer de una disponibilidad del 99,9%.

- *Servicio Público Regulado*, dedicado a aplicaciones específicas sobre los países de la UE, como pueden ser las relacionadas con la seguridad, policía, protección civil, servicios de emergencia etc.

- *Servicios proporcionados por elementos locales*, los cuales logran precisiones de posicionamiento de entre un metro y diez centímetros.

- Servicios de búsqueda y rescate, coordinados con los actuales COSPAS-SARSAT[9], compatibles con GMDSS[10] y la red de transporte transeuropea, permitiendo mejorar la detección y precisión de localización de las balizas disponibles en relación con

[9] En la actualidad, el sistema LEOSAR de navegación aérea consta de un mínimo de cuatro satélites, dos "tipo Cospas" y dos "Sarsat", ofreciendo una capacidad de vigilancia que comprende prácticamente todo el planeta (el tiempo de espera para la localización de cualquier posición bajo un plano orbital resulta inferior a una hora para latitudes medias). Rusia opera con el sistema COSPAS, y Estados Unidos suministra los satélites SARSAT.

Las señales emitidas desde estos satélites son recibidas en unas estaciones locales denominadas LEOLUT. A modo ejemplar, en España contamos con la LUT de Maspalomas, que cubre no solo el territorio nacional sino además Marruecos, Argelia, Túnez, Camerún, Níger, Burkina-Faso y parcialmente Libia y Chad, en África; y Andorra, Bélgica, Francia, Irlanda, Italia, Luxemburgo, Malta, Mónaco, Portugal, Suiza y parcialmente Alemania, Austria y Reino Unido, en Europa.

Vid., AGENCIA ESTATAL DE SEGURIDAD AÉREA. *Programas de navegación aérea. Cospas-Sarsat.* Ministerio de Fomento. Gobierno de España. Recuperado de: http://www.seguridadaerea.gob.es/lang_castellano/navegacion/programas/cospas/descripcion/default.aspx (última consulta: 4 de abril de 2016).

[10] GMDSS o *Global Maritime Distress Safety System* (Sistema Mundial de Socorro y Seguridad Marítima).

los sistemas actuales, lo cual favorece el paso de la actual precisión de 5 km a 10 metros, para las balizas equipadas con receptores Galileo.

El GPS funciona mediante la determinación de distancias a través de puntos móviles, que son los satélites, mediante una triangulación[11].

I.2.- Datos de geolocalización de estaciones base tratados por operadores de telecomunicaciones

Existen otras aplicaciones que permiten la navegación sin necesidad de hacer uso de los satélites del sistema GPS, y ello valiéndose precisamente del aporte de información sobre localización que puede obtenerse de puntos fijos, tales como las estaciones base (o estaciones BTS) o redes o dispositivos *WiFi* de los que se sirven los terminales, tipo telefonía móvil, tabletas o *smartphones*, para prestar servicios de localización. La información cartográfica accede al terminal por Internet en función de su localización geográfica; el terminal se posiciona mediante triangulaciones de referentes fijos, con los que dialoga automáticamente.

[11] El receptor GPS recibe información que se estructura en dos tipos: a) "almanaque" o serie de parámetros referidos a la ubicación y operatividad de los distintos satélites que configuran la red, y b) "efemérides" o datos precisos del satélite que ubican al satélite en su órbita, y son empleados por el receptor GPS para determinar la distancia exacta receptor-satélite.

Vid., LUQUE SOTO, R., "Uso policial y análisis forense de información de aplicaciones móviles para localización de personas de interés", (Dtor.) MONTOYA MARTÍ, A., CUGC, Aranjuez, 24 de mayo de 2016, p.36.

Las posibilidades que ofrece el mercado en este punto son amplísimas; abarca desde interactuaciones con sistemas *Google Earth*, hasta la posibilidad de uso alternativo de la navegación GPS o GSM según las mayores prestaciones o mejor calidad del servicio en cada momento y lugar determinados, pasando por interrelación de datos GPS, incluso mejorados, vía Internet, con la prestación de servicios de navegación por este último canal de comunicaciones (cálculo de rutas y distancia, tiempo previsto del viaje, puntos de interés, información atmosférica y sobre tráfico, etc.).

En cuanto a la telefonía móvil, tenemos que indicar que se apoya en la inclusión del concreto equipo terminal en el área ("celda") cubierta por una determinada antena de telefonía (o satélite, en su caso) encargada de enviar la señal, a efectos de realizar la eventual comunicación telefónica, la cual cambia al desplazarse el usuario y ubicarse en el área cubierta por una celda distinta. Así, cuando un teléfono móvil se conecta a la red GSM, su localización geográfica (*Location Area*) queda almacenada en un registro de la compañía operadora, el HLR (*Home Location Register*). Esa posición se irá actualizando permanentemente, con independencia de que se esté efectuando o no una comunicación, sin que el usuario perciba señal alguna al encontrarse conectado de manera permanente, cuando el dispositivo móvil está encendido con una determinada estación base, la

cual ostenta un número de identificación único y se encuentra registrada con una ubicación específica.

Tanto el operador de telecomunicaciones, como muchos dispositivos móviles son capaces de utilizar las señales de casillas (estaciones base) solapadas para estimar la posición del dispositivo móvil con mayor precisión, y para ello se ayudan de diversas técnicas:

- La *triangulación*, la cual utiliza ángulos para determinar la posición de un nodo[12] o antena. En general, se requieren dos ángulos y la distancia entre dos puntos de referencia en un entorno bidimensional. Sin embargo, para tres dimensiones son necesarios dos ángulos, la distancia entre dos nodos de referencia y un azimut[13] para especificar una posición precisa. Normalmente se utiliza un vector de referencia constante con valor 0° (por ejemplo, el norte magnético). Esta técnica hace uso de varios nodos fijos cuya posición es conocida. Cada nodo fijo ha de ser capaz de determinar la dirección (ángulo) en la que se encuentra el punto determinable. Si hay suficientes elementos en la red de antenas y suficientes separaciones, se puede realizar el cálculo de la triangulación.

[12] En la red de comunicaciones se despliegan físicamente nodos por toda la geografía para ofrecer el servicio a los clientes de la operadora. La operadora dispone de la información de la localización exacta de todos sus nodos o antenas que han sido desplegados por un área geográfica con, por supuesto, las coordenadas geográficas de todos ellos.

[13] Ángulo que, con el meridiano, forma el círculo vertical que pasa por un punto de la esfera celeste o del globo terráqueo.

La precisión en la localización puede incrementarse con la ayuda de parámetros como la intensidad de la señal recibida, la diferencia en el tiempo de llegada de la señal y el ángulo de entrada de la señal[14]. En cualquier caso, la precisión es de aproximadamente 50 metros en las zonas urbanas densamente pobladas y de hasta varios kilómetros en las zonas rurales.

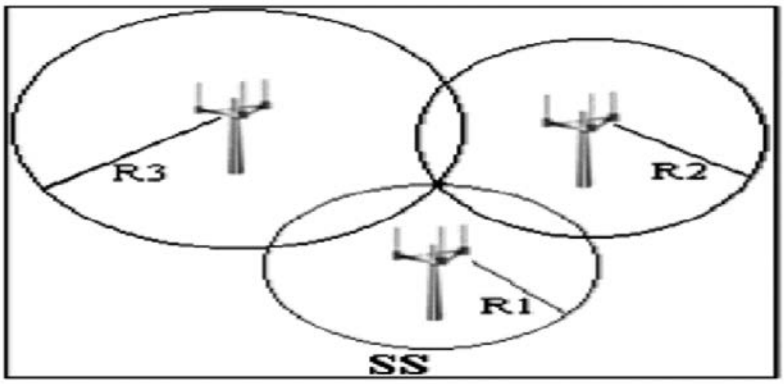

Ilustración 1: Triangulación*¡Error! Marcador no definido.*

- La *trilateración*, que es similar a la anterior, con la diferencia de que, en vez de ángulos, se usan distancias para determinar la posición de un nodo. Para calcular la posición de un dispositivo móvil en dos dimensiones es necesario conocer al menos las distancias desde tres nodos en diferentes líneas (dos circunferencias que interseccionan lo hacen en uno o dos puntos); un tercer nodo describe una tercera circunferencia que determina

[14] *Vid.,* UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29, Dictamen 13/2011…*op.cit.*, p.4-5.

el punto donde se encuentra el terminal móvil. En tres dimensiones, serían necesarios cuatro nodos en planos distintos.

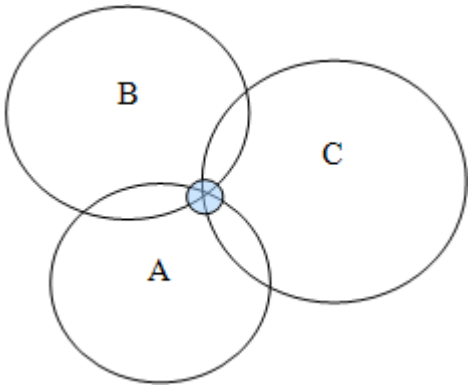

Ilustración 2: Trilateración

- La *multilateración*, también llamada posicionamiento hiperbólico, es una técnica que emplea la magnitud TDOA[15] para el posicionamiento tridimensional de una estación móvil mediante un mínimo de 4 antenas. Conociendo la posición de 2 antenas (las cuales ya no necesitan ser unidireccionales) y conociendo el TDOA de una señal proveniente de la MS que se quiere localizar, el problema de búsqueda del punto emisor se reduce a localizarlo en el interior de un hiperboloide de dos hojas. Añadiendo un tercer nodo de medición se obtiene una nueva diferencia de tiempos de llegada, lo que genera un nuevo hiperboloide que intersecciona con el anterior, reduciendo el problema a una curva en la superficie de una de las dos hojas del hiperboloide. Si añadimos una cuarta antena, obtenemos un nuevo TDOA y generamos un nuevo hiperboloide. Dicho hiperboloide intersecciona con los otros dos (o

[15] TDOA o *Time Difference of Arrival*, consistente en la medición de la diferencia de tiempo de llegada de las diferentes señales.

con la curva generada por la intersección de los dos primeros) en un único punto común, que es el punto que hay que determinar. En este caso, se da también la coordenada de altura del punto de medición.

- La *parametrización*, que contrasta ciertos parámetros únicos para una región geográfica (previamente medidos y almacenados en una base de datos) que se están tomando en un instante determinado en el terminal móvil. Se realiza en la zona cercana a las antenas BTS. Para el buen funcionamiento de este método, bajo una región geográfica de interés se han de tomar todas las mediciones que la red GSM pueda proporcionar (CellID, TA, potencia…). De esta manera, se genera una base de datos que contiene coordenadas expresadas en latitud y longitud, con la precisión que deseemos, relacionadas con la zona a estudio[16]. Una vez el usuario del terminal móvil inicie la aplicación de geoposicionamiento, el sistema comprueba a qué coordenada se parece más la medición actual y, por tanto, devuelve la coordenada aproximada si la medición actual es coincidente con la almacenada, o bien interpola la coordenada teniendo en cuenta las registradas en la proximidad. La dificultad de este método estriba en la generación de la base de

[16] La precisión de este sistema de localización es directamente proporcional al número de puntos en los que se realicen las mediciones con las que se alimenta el servidor.

datos y su tamaño, pues puede exceder la capacidad de almacenamiento de un terminal móvil[17].

Más concretamente, en los *smartphones* o *tablets*, los datos de localización se generan mediante la conservación de unos datos que se transmiten de forma automática entre la estación BTS de referencia y el terminal telefónico a ella asociado, cada vez que se emite o recibe una comunicación, no gozando éstos de la naturaleza de dato de tráfico[18]. El canal de control que relaciona terminal y estación BTS da pie a la emisión por el primero de una señal que identifica a este, y a su vez, gracias al apoyo de los canales de difusión, a la emisión de otras señales que interconectan al terminal con otras estaciones BTS en su radio de alcance, con la finalidad concreta de asegurar la continuidad y calidad de la señal de la comunicación en caso de pérdida o deficiencia de la facilitada por la estación BTS de referencia.

En los CDR (*Call Data Record*) queda registrada la posición de la estación base inicial, pudiendo conocerse las siguientes estaciones a través de la base de datos VRL (*Visitor Location Register*), de modo que esta información de actualización de la posición geográfica queda

[17] HERNANDO RABANOS, J.M., "Comunicaciones móviles", 2ª edición, Editorial Universitaria Ramón Areces, Madrid, 2004.

[18] Podemos avanzar, aunque posteriormente lo desarrollaremos, la tesis de RODRÍGUEZ LAÍNZ consistente en afirmar que estos datos no ostentan la naturaleza de dato de tráfico.

Vid., RODRÍGUEZ LAÍNZ, J.L., *Internet de los objetos y secreto de las comunicaciones*, Diario La Ley, núm. 8034, Sección Doctrina, Año XXXIV, Ref. D-85, Editorial LA LEY, 1 de marzo de 2013.

registrada temporalmente durante un breve lapso de tiempo (dependiendo del operador); en España ronda las 72 horas[19].

Partiendo de lo anterior, existen, además, procedimientos que, empleando medios adicionales a los propios de la red celular y basándose igualmente en la radiogoniometría, nos permiten obtener datos aún más exactos de localización. Estamos hablando de las "falsas estaciones BTS" usadas actualmente, como veremos en el siguiente capítulo, por las Fuerzas y Cuerpos de Seguridad del Estado para la localización de un dispositivo electrónico, existiendo incluso resoluciones judiciales al respecto. Estas estaciones simulan en la interfaz de radio, ser una celda que ofrece mayor potencia de red, conectándose así los dispositivos electrónicos (debido a que éstos están programados para que traten de registrarse en aquellas estaciones base que mejores condiciones de potencia de señal ofrecen, para así lograr ahorro de energía y contar con mejor conexión). Una vez que el terminal se registra en estas estaciones base móviles, se obtiene el control del mismo, al igual que lo hace una BTS fija, de modo que se puede adjudicar la frecuencia y el canal exacto de subida en el que se quiere que transmita, monitorizando con ello, a través del radiogoniómetro, el punto exacto del que procede la emisión de radio del dispositivo electrónico y con ello su localización exacta en el espacio.

[19] En la sentencia de la Audiencia Nacional, Sala de lo Penal, 65/2007, de 31 de octubre, caso 11-M, expresamente se hace constar que *"La información sobre dónde ha estado "acampado" un determinado teléfono se mantiene durante 72 horas en las correspondientes centrales de conmutación, de modo que si un teléfono está apagado o fuera de cobertura la información sobre cuándo y dónde estuvo encendido la última vez no desaparece de inmediato, sino que se conserva durante este periodo temporal".*

Para el cálculo de una posición, como se ha visto, existe un número determinado de BTS con una posición determinada y fija. La ventaja de esta "falsa estación BTS" precisamente reside en su movilidad, de modo que puede ir realizando mediciones sucesivas y cambiando de posición sobre la marcha, siendo capaz de detectar la dirección con la que se recibe la transmisión de radio del dispositivo y su potencia de llegada con la ayuda de un radiogoniómetro[20].

En cuanto a sus inconvenientes, se hace preciso conocer los datos de identificación del dispositivo electrónico que se pretende localizar (IMSI e IMEI[21], así como el proveedor de servicios de comunicaciones móviles al que está suscrito), ya que existirán una multiplicidad de ellos interactuando en la red y se ha de poder distinguir de los restantes[22].

[20] Según el Diccionario de la Lengua Española de la Real Academia Española, podemos definir "radiogoniómetro" como "*1. m. Electr. Aparato receptor que permite determinar la dirección de una señal radioeléctrica.*"

Vid., REAL ACADEMIA ESPAÑOLA. Diccionario de la Lengua Española. Recuperado de: http://www.rae.es (última consulta: 14 de mayo de 2013).

[21] El término IMSI es el acrónimo de *International Mobile Subscriber Identity*. Se trata de un código de identificación único para cada dispositivo de telefonía móvil, representado por una serie de algoritmos, integrado en la tarjeta SIM (*Subscriber Identity Module*), que se inserta en el teléfono móvil para asignarle el número de abonado o MSISDN (*Mobile Station Integrated Services Digital Network*) y que permite su identificación a través de las redes GSM y UMTS.

Otro identificativo asociado al teléfono móvil es el IMEI o *International Mobile Equipment Identity* (Identidad Internacional del Equipo Móvil), que identifica con su número de serie al equipo.

Vid., RODRÍGUEZ LAÍNZ, J.L., *Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas*, Diario LA LEY, núm. 7086, Sección Doctrina, Año XXIX, Editorial LA LEY, 2 enero de 2009.

[22] Como explica VALLÉS, *"[…] La información, por tanto, es referida a tantos IMSI e IMEI como personas y terminales estén en el momento del rastreo registrados en el aparato a efectos de tener cobertura. De esta manera, se sabe cuál es el IMSI e IMEI objeto de interés de la investigación, pero únicamente por la mera exclusión de los demás números IMSI e IMEI no sospechosos y no captados de nuevo cuando vuelve a hacerse un rastreo en los diferentes lugares en los que el sospechoso sucesivamente se halla".*

Vid., VALLÉS CAUSADA, L. M., "La policía judicial en la obtención de inteligencia sobre comunicaciones electrónicas para el proceso penal", Tesis Doctoral, (Dtor.) DÍAZ MARTÍNEZ, M., UNED, Madrid, diciembre 2012, nota a pie 766, p.352.

Además, dado que estas "falsas BTS" cuentan con una potencia de señal de radio reducida, es necesario tener conocimiento previo de la localización aproximada del dispositivo electrónico, ya que de otro modo no se podrán recibir sus señales de radiofrecuencia.

Ubicado el radiogoniómetro en la zona previamente determinada, este equipo estará preparado para efectuar muestreos en diferentes ubicaciones hasta detectar al dispositivo electrónico que se pretende localizar, y a partir de ahí, se verificarán sucesivas operaciones similares para ir determinando la ubicación en todo momento.

Aparte, en prácticamente todos los terminales móviles de comunicaciones existen aplicaciones informáticas que pueden ser ejecutadas por el usuario (empleando conectividad IP y tráfico de datos) y que utilizan datos relativos a la localización del terminal para prestarle multitud de servicios. Actualmente la mayoría de los dispositivos cuentan con tecnología GPS, lo que les lleva a poder calcular su posición con precisión muy alta y con márgenes de error menores de 15 metros[23].

I.3.-Redes WiFi

[23] A modo ejemplar, *Foursquare* para localizar a amigos y poder enviarles nuestra posición, *Cell Tracker*, que realiza un seguimiento de la ubicación del celular, *Teen Safe* o *My Mobile Watchdog*, dedicadas al control parental, que monitorean, entre muchas otras opciones, el punto exacto en el que está el teléfono.

Una fuente de información, a efectos de geolocalización, relativamente nueva es el uso de los puntos de acceso *WiFi*[24]. La tecnología es similar al uso de estaciones de base. Ambas se valen de un número de identificación único de la estación de base o del punto de acceso *WiFi,* que, según cada caso, puede ser detectado por un dispositivo móvil y enviado a un servicio que conoce la ubicación de cada uno de estos puntos de identificación únicos[25].

Más concretamente, las formas de recopilar las direcciones MAC[26] de los puntos de acceso *WiFi* son[27]:

- Barrido activo o envío de solicitudes activas a todos los puntos de acceso *WiFi* cercanos con registro de sus respuestas, las cuales no incluyen información sobre los dispositivos conectados a ese punto de acceso.

[24] *Vid.* UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 de la Directiva 95/46/CE, Dictamen 13/2011..., *op.cit.*, p.5-6.

[25] La identificación única de cada punto de acceso *WiFi* es su dirección de control de acceso al medio ("dirección MAC" o *Medium Access Control*). La dirección MAC es un identificador único asignado a una interfaz de red, y normalmente registrada en componentes como microprocesadores de memoria o tarjetas de red en ordenadores, teléfonos, ordenadores portátiles o puntos de acceso.

[26] MAC son las siglas de *Media Access Control* y se refiere al control de acceso al medio físico. La dirección MAC es una dirección física (también llamada dirección hardware), alojada en las tarjetas de red tipo Ethernet (ya de fábrica) y formada por 48 bits que se suelen representar mediante dígitos hexadecimales que se agrupan en seis parejas (a modo ejemplar, "F0:E1:D2:C3:B4:A5"). Esta dirección, única para cada tarjeta, permite las transmisiones de datos entre ordenadores de la red, puesto que cada ordenador es reconocido mediante esa dirección MAC, de forma inequívoca.

[27] De conformidad con el Standard IEEE 802.11 Wireless Lan (WLAN), es una frecuencia de radio desarrollada por el *Institute of Electrical and Electronics Engineers* y es soportada por la mayoría de los sistemas operativos existentes en portátiles, móviles de última generación, impresoras y demás periféricos, consolas, etc.

Vid., INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. Recuperado de: https://www.ieee.org/index.html (última consulta: 17 de julio de 2013).

- Barrido pasivo o registro de las señales transmitidas periódicamente por cada punto de acceso (generalmente 10 veces por segundo).

La ubicación de un punto de acceso puede calcularse de dos formas diferentes:

- Estáticamente y una sola vez; así los responsables del tratamiento de datos recopilan las direcciones MAC de los puntos de acceso *WiFi* desplazándose con vehículos equipados con antenas; se registran la latitud y la longitud exactas del vehículo y el momento en que se recibe la señal; así se puede calcular la ubicación de los puntos de acceso utilizando, entre otros datos, la intensidad de dicha señal.

- Dinámica y continuamente; así los usuarios de servicios de geolocalización recogen automáticamente las direcciones MAC captadas por sus dispositivos *WiFi* cuando, por ejemplo, utilizan un mapa en línea para determinar su propia posición. El dispositivo móvil envía toda la información disponible al proveedor del servicio de geolocalización, incluida la dirección MAC, las SSID[28] y la intensidad de señal. El controlador puede usar estas consultas en

[28] El llamado identificador de conjunto de servicios (siglas en ingles SSID o *Service Set Identifier*) es el nombre único de una concreta red inalámbrica. Por defecto, el SSID generalmente es determinado por el adaptador o *router* inalámbrico que el usuario utiliza, y está compuesto por cualquier combinación de caracteres de ASCII (es decir, cualquier combinación de letras, números, signos de puntuación, etc.).

curso para calcular o mejorar la localización de los puntos de acceso *WiFi* en su base de datos.

En resumen, los puntos de acceso *WiFi* pueden ser utilizados como una fuente de información a efectos de geolocalización ya que anuncian continuamente su existencia. Al igual que una radio, un punto de acceso *WiFi* transmite continuamente su propio nombre de red y su dirección MAC, incluso cuando nadie esté utilizando la conexión o cuando este contenido de las comunicaciones inalámbricas esté cifrado mediante WEP, WPA o WPA2[29]. Por otro lado, los dispositivos móviles no necesitan "conectarse" a puntos de acceso *WiFi* para recoger información *WiFi*, ya que detectan automáticamente la presencia de dichos puntos (en modo de barrido activo o pasivo) y automáticamente recogen datos sobre ellos. Aún es más, los teléfonos móviles que soliciten ser geolocalizados no solo enviarán datos *WiFi*, sino también, a menudo, cualquier otra información sobre localización de la que dispongan, incluidos los datos sobre GPS y estaciones de base.

I.4.- Sistema Silent

[29] WEP o Wired Equivalent Privacy (Privacidad Equivalente a Cableado), era un sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permitía cifrar la información que se transmitía. Posteriormente surgió WPA o *WiFi Protected Access*, creado para corregir las deficiencias del anterior. WPA2 es una versión mejorada del anterior.

Otra opción con la que cuentan las unidades de investigación[30] para la localización de un teléfono en un momento determinado, consiste en provocar una comunicación a través de un mensaje de texto o "*SMS* silencioso". Estos *SMS* invisibles fueron creados inicialmente para que las operadoras móviles pudieran confirmar si un determinado teléfono se encontraba encendido, así como para poder realizar comprobaciones en la red[31].

El Sistema *Silent,* también denominado Flash-SMS, utiliza una señal de retorno invisible o "ping". Este sistema permite acreditar la localización de personas a través del envío de un mensaje que en ningún caso recibirá el usuario del terminal móvil y que, sin embargo, sí habrá quedado archivado, como acto de comunicación entre los datos que posee la operadora de telecomunicaciones, de manera que posteriormente podrán ser recabados.

[30] Como muestra de uso generalizado por parte de las unidades de investigación, en Alemania la diputada Anna Conrads planteó en el Parlamento regional de Renania-Westfalia una pregunta sobre la utilización de este sistema por parte de la policía alemana, obteniendo como respuesta que, durante el año 2010, se enviaron 256 mil SMS silenciosos en el curso de 778 investigaciones. Por su parte, el Ministro del Interior alemán, en diciembre de 2010, confirmó el envío de 440 mil SMS silenciosos, de media, cada año.

HEISE ONLINE. Recuperado de: http://www.heise.de/newsticker/meldung/Zoll-BKA-und-Verfassungsschutz-verschickten-2010-ueber-440-000-stille-SMS-1394593.html (última consulta: 13 de marzo de 2014).

[31] Los desarrolladores de la firma Silent Services, creadora del primer software para el envío de estos SMS, afirman que: "*El Silent SMS permite al usuario enviar un mensaje a otro teléfono móvil sin que el propietario de éste lo sepa. El mensaje es rechazado por el móvil de destino y no deja ningún rastro en él. En respuesta, el remitente recibe un mensaje de la operadora móvil confirmando la recepción del SMS invisible"*

Vid., SILENT SERVICES. Recuperado de: http://www.silentservices.de (última consulta: 2 de febrero de 2015).

I.5.- Tarjeta SIM, fichero LOCI

Dentro de la tarjeta SIM de cada dispositivo electrónico se encuentra el fichero LOCI, de particular relevancia para la investigación, pues entre otras informaciones contiene el *Location Area Identifier* (LAI), o un indicativo del último lugar donde se halla el móvil. Este dato queda almacenado en la SIM en el momento en que se desconecta el teléfono, por lo que permite saber en qué área o zona geográfica se encontraba el teléfono cuando operó por última vez. Si al pulsar el botón de encendido, el móvil se encontrase en la misma área, refresca el contenido de estos ficheros para empezar a operar, pero si se halla en otra diferente, se actualizará.

La localización en virtud del LAI quizá no sea demasiado precisa, puesto que puede referirse a muchas celdas, incluso cientos de ellas dependiendo del lugar donde se encuentre. De ahí que la determinación del lugar exacto donde estuvo por última vez el teléfono probablemente no esté guardada en la SIM, sino que será el operador quien la conserve registrada y quien, por ende, estará en disposición de cederla de ser preciso, entrando de lleno en el ámbito de protección del artículo 18.4 de la Constitución Española.

I.6.- Archivos Exif

Los archivos *Exif* (sigla inglesa de *Exchangeable image file format*), incluidos en las fotografías digitales, pueden suministrar información sobre el dispositivo móvil con el que se creó, sobre el tipo de cámara y tiempo de exposición, sobre el nombre de la versión del software con la que se editó la imagen y sobre otros muchos datos; aporta igualmente las coordenadas geográficas donde es tomada la foto cuando el dispositivo tiene capacidades de GPS, por ejemplo *smartphones* como el *IPhone*[32].

I.7.-Peculiaridades de la vigilancia discreta –balizas-

No podemos olvidarnos de las denominadas *balizas* o modalidad dinámica de localización, donde se integran distintos avances tecnológicos; existen las que utilizan GPS, las basadas en módulos de satélite independientes (sistema Alpha), las basadas en radiofrecuencia,

[32] Diversos *smartphones* guardaban inicialmente información geográfica sobre los lugares donde han estado, así como la de los puntos de acceso *WiFi* que han detectado. Por ejemplo, en el *IPhone*, un fichero denominado "consolidated.db" almacena todos los datos registrados por el dispositivo en lo que a geolocalización se refiere. Los archivos electrónicos que se generaban estaban muy poco protegidos y, por ende, eran vulnerables, permitiendo que información tan sensible como la de la geolocalización se desplazara por la red sin estar cifrada, y sin consentimiento del titular. Este problema era común a seis fabricantes de sistemas operativos móviles: Google, Apple, Nokia, Microsoft, RIM y HP, lo que obligó al Grupo de Trabajo del artículo 29 o autoridad europea de protección de datos, a publicar un dictamen recomendando que los teléfonos móviles y las tabletas se ofrecieran al cliente con el servicio de geolocalización desactivado, debiendo éste ponerlo en funcionamiento de manera consciente, otorgando con ello su consentimiento.

Vid., UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29, Dictamen 13/2011 op.cit.

Vid., PÉREZ GIL, J., *El nuevo papel de la telefonía móvil en el proceso penal: ubicación y perfiles de desplazamiento*, en PÉREZ GIL, J. (Dtor.) "El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito", Editorial LA LEY, Madrid, 2012, nota 61.

las basadas en la comunicación de GSM (telefonía móvil) y los dispositivos de descarga de localización (Qlog)[33].

El control permanente de los movimientos de la persona se realiza con carácter mediato, pues la deducción de su posición proviene de la señal enviada por un dispositivo colocado en el entorno del sujeto monitorizado que sigue sus desplazamientos; esa señal puede ser recibida por los investigadores a través de diversas vías, en función de la tecnología empleada (red GSM, radiofrecuencia, sistemas satelitales especiales, etc.). Puede tratarse de los instrumentos tecnológicos de que habitualmente se sirve la persona (caso del teléfono móvil) o elementos que los autores de la investigación introducen subrepticiamente en su entorno (*beeper*, GPS, etc.) y que periódicamente envían las señales que permiten ubicarla, estando escondido en un medio de transporte que use la persona, en un objeto que se le ha proporcionado, en una prenda de vestir, etc.

Estas balizas pueden gestionarse en remoto, variando su configuración, para adaptarse a las cambiantes necesidades de la investigación.

I.8.-Geolocalización a través de direcciones IP

[33] LLAMAS FERNÁNDEZ, M. Y GORDILLO LUQUE, J. M., *Medios técnicos de vigilancia*, en VELASCO NÚÑEZ, E. (Dtor.), "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia", Consejo General del Poder Judicial, Madrid, 2007, p. 227-230.

La dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (un ordenador, un *smartphone* etc.) dentro de una red que utilice el protocolo IP (*Internet Protocol*[34]).

Para individualizar los millones de ordenadores existentes, se utiliza esta dirección IP, la cual está compuesta por cuatro grupos de números, del 0 al 255, separados por puntos. Por tanto, la dirección IP no es más que un código de números de 32 bits que permite el establecimiento de una comunicación entre dos terminales informáticos o *hosts*. Esta dirección IP es única y exclusiva para cada conexión, en el sentido de que no se puede acceder desde ningún ordenador a Internet sin tener adjudicada una dirección IP y no puede existir, al mismo tiempo, dos conexiones a Internet con la misma dirección IP.

La dirección IP es un recurso escaso, con un número total disponible de cuatro mil millones de direcciones en todo el mundo; el organismo llamado ICANN (*Internet Corporation for Asigned Names and*

[34] *Internet Protocol* (en español 'Protocolo de Internet') o IP es un protocolo de comunicación de datos digitales, clasificado funcionalmente en la Capa de Red según el modelo internacional OSI. Su función principal es el uso bidireccional, en origen o destino, de comunicación para transmitir datos mediante un protocolo no orientado a conexión, que transfiere paquetes conmutados a través de distintas redes físicas previamente enlazadas, según la norma OSI de enlace de datos.

Numbers) es la autoridad internacional encargada de definir los procedimientos y requisitos para delegar el uso de direcciones IP[35].

Los IPs pueden ser fijos o dinámicos. Los operadores asignan direcciones IP libres a aquellos clientes que precisen conectividad en un momento concreto (direccionamiento dinámico); por el contrario, en el estático, el cliente, esté conectado o no, siempre tiene la misma dirección IP. Actualmente, los IPs fijos son raros debido a razones de seguridad, ya que los ataques son más fáciles cuando el número de identificación de un terminal es siempre el mismo[36].

En cualquier caso, los números asignados como IP no son escogidos al azar; dependen del tipo de conexión que se utilice y del lugar desde donde se conecte el usuario, asignándose rangos de direcciones IP

[35] "*A nivel mundial existen 5 organismos regionales que ejecutan las directrices del ICANN en su región. La función más relevante es la asignación de direcciones IP. Cada uno de estos organismos dispone de un servicio (who is?) de consulta pública y gratuita, que permite obtener los datos del adjudicatario de una dirección IP y la forma de contacto.*

El organismo europeo responsable de ejecutar las directrices del ICANN se llama RIPE (Résseaux IP Européens). Este organismo es el que delega el uso de direcciones IP a los ISPs (proveedores de conectividad IP etc), que deben satisfacer el pago de una cuota anual que dependerá del volumen de direcciones que contratan. La clave de la delegación es el uso responsable de un recurso escaso, por tanto, los operadores tendrán que justificar la necesidad de las IP´s que solicitan".

Vid., MARTÍNEZ GINESTA, G., *Límites técnicos de la ayuda prestada por las operadoras en la investigación de los delitos,* en VELASCO NÚÑEZ, E., "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia", Consejo General del Poder Judicial, Madrid, 2007, p. 114.

[36] La rotación de direcciones IPs (IP dinámicos) funciona de la siguiente forma: un determinado proveedor de acceso a Internet (Ej. Arnet), posee X números IPs para usar. Cada vez que una máquina se conecta a internet, el proveedor le asigna una dirección IP aleatoria, dentro de una cantidad de direcciones IPs disponibles. El proceso más utilizado para esta distribución de IPs dinámicos es el Dynamic Host Configuration Protocol (DHCP). Para acceder a las URLs, o direcciones IPs públicos como conocemos (p.ej. www.boe.es), existen los servidores DNS (Domain Name Server, en inglés), una base de datos responsable por la traducción de nombres alfanuméricos a direcciones IP, fundamentales para el funcionamiento de Internet tal como la conocemos hoy.

por zonas geográficas de forma ordenada, por lo que el servidor[37] con el que se establezca una conexión, puede identificar aproximadamente el área desde donde se le efectúa la petición o lo que es lo mismo, la geolocalización del usuario.

I.9.-Etiquetas inteligentes con tecnología **WiFi**

El crecimiento de Internet es un fenómeno actual de imposible negación. Hace solo veinticinco años conectaba a un millar de ordenadores y desde entonces, ha crecido hasta enlazar a miles de millones de personas a través de ordenadores y dispositivos móviles. Crucial, en este avance, es la evolución progresiva de una red de ordenadores interconectados, a su vez, a una red de objetos también interconectados (desde libros, hasta automóviles, aparatos electrodomésticos, alimentos…); se ha creado así la *Internet de los Objetos* (IO)[38].

[37] Servidor entendido como *"equipo informático al que se ha dotado de información o de software y al que pueden acceder sus usuarios. Los servidores han de estar conectados permanentemente a Internet, ya que es la única manera de poder ser accesibles por los clientes."*.

COZAR BARREIRO, J., *Delincuencia informática: conceptos básicos y posibilidades de investigación*, en "Interceptación de las comunicaciones y nuevas tecnologías", Cuadernos Digitales de Formación, núm. 43, Consejo General del Poder Judicial, 2010, p.5.

[38] INTERNATIONAL TELECOMMUNICATION UNION, *The Internet of Thing,* ITU Internet Report, noviembre de 2005. Recuperado de: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf (última consulta: 6 de marzo de 2015).

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación -TIC-. La UIT fue fundada en París, en 1865, con el nombre de Unión Telegráfica Internacional. En 1934 adoptó su nombre actual y, en 1947, se convirtió en organismo especializado de las Naciones Unidas. Como organización basada en la asociación público-privada desde su creación, la UIT cuenta en la actualidad con 193 países miembros y más de 700 entidades del sector privado e instituciones académicas. La UIT tiene su Sede en Ginebra (Suiza) y cuenta con 12 oficinas regionales y de zona en todo el mundo.

Se puede definir la Internet de los Objetos (IO) como redes de objetos etiquetados interconectados que establecen enlaces entre la naturaleza física de tales objetos (por ejemplo, localización, situación, actividades, comportamiento, propiedad) y la información en línea relacionada con ellos, que se facilita continuamente mediante una red de sensores. La interactuación es tal, que cabe la posibilidad de implicar auténticas decisiones humanas con el constante flujo de información y decisiones automáticas que adopta el propio sistema[39].

Tres puntos ponen de relieve la compleja naturaleza de la Internet de los Objetos[40]:

1.- No ha de verse como una mera extensión de la actual Internet, sino como una serie de nuevos sistemas interdependientes que operan con sus propias infraestructuras (basándose, en parte, en las ya existentes de Internet).

2.- La IO se pondrá en práctica en simbiosis con nuevos servicios[41].

[39] RODRÍGUEZ LAINZ, J.L., "Estudios sobre el secreto de las comunicaciones. Perspectiva doctrinal y jurisprudencial", 1ª edición, Editorial LA LEY, Madrid, 2011, p. 55-48.

[40] COMISIÓN EUROPEA, Comunicación de la Comisión al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, "Internet de los objetos-plan de acción para Europa" (COM (2009/278) final), de 18 de junio de 2009. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Asi0009 (última consulta: 12 de diciembre de 2016).

[41] MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL, Informe del Grupo Asesor del programa de Tecnologías de la Sociedad de la Información (ISTAG), febrero de 2009.

3.- La IO abarca diferentes modos de comunicación: comunicación de objetos con personas y comunicación de objeto con objeto, incluida la comunicación de máquina con máquina; la capacidad de conexión es de 50 mil a 70 mil millones de máquinas; de ellas solo el 1% están conectadas en la actualidad[42].

La IO llega a un entorno informático en el influyen varias tendencias fundamentales[43]. Una de ellas es la "escala", dado que el número de dispositivos conectados está aumentando, mientras que su tamaño se reduce, además de la "movilidad", estando los objetos cada vez más conectados de manera inalámbrica, y siendo transportados permanentemente por las personas, aparte de ser geolocalizables, y por último, la "heterogeneidad y complejidad" al desarrollarse en un entorno ya abarrotado de aplicaciones, lo cual genera cada vez más dificultades de interoperabilidad.

Desde el punto de vista técnico, un amplio conjunto de tecnologías participará en la consolidación de la IO. El desarrollo de la infraestructura de redes de comunicación a través de redes de banda ultraancha y redes 3G y 4G, será fundamental, así como la instauración de IPv6 que permitirá otorgar una dirección IP única a cada objeto que

[42] Esta es la cifra manejada habitualmente por diferentes autores que parten del supuesto de que cada persona está rodeada en promedio por unas diez máquinas.

[43] Comunicación de la Comisión de 29 de septiembre de 2008 al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, "Comunicación sobre las redes y la Internet del futuro" (COM/2008/594 final), de 29 de septiembre de 2008. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Asi0003 (última consulta: 17 de julio de 2015).

participe en la red. Las tecnologías que permitan tanto la localización como la identificación de los objetos físicos serán también básicas en este contexto. Existen además tecnologías que pueden influir en el funcionamiento de la IO como, por ejemplo, la visión por computador, los sistemas biométricos, la robótica y otros. Sin embargo, dentro de la conexión de los objetos con la infraestructura de los sistemas de información, dos son las tecnologías clave que cuentan con madurez y calado bastante como para acercar la IO a la realidad: la identificación por radiofrecuencia (RFID) y las redes de sensores inalámbricas[44].

Como dice RODRÍGUEZ LAÍNZ[45], nos encontramos en un mundo en el que las máquinas e incluso simples objetos, interactúan entre sí, a través de las redes de comunicaciones electrónicas, compartiendo o transmitiendo información, que es procesada, dando lugar a decisiones igualmente automáticas, a veces, a miles de kilómetros de distancia.

---

[44] *"La tecnología RFID permite identificar de manera univoca a un objeto y obtener información sobre él o su entorno gracias a los datos transmitidos de manera inalámbrica por una etiqueta RFID incorporada en el mismo. […] No obstante, las prometedoras cualidades de la tecnología RDIF la convierten en un arma de doble filo, principalmente debido a las amenazas a la privacidad e intimidad (p.e. creación de perfiles sobre individuos, seguimientos no autorizados) y a la extremada baja capacidad de las etiquetas RFID."*

"Metafóricamente hablando, una red de sensores puede considerarse como la "piel" de un sistema computacional, la cual es capaz de percibir las características físicas del entorno. En vez de "células", las redes de sensores están compuestas de una serie de dispositivos conocidos como nodos sensores o simplemente nodos, los cuales normalmente están limitados en términos de velocidad de procesamiento (hasta 32MHz) y memoria (hasta 256KB). Su principal tarea es la de "sentir", es decir, obtener información del entorno a través de medidores de temperatura, humedad, radiación y otros. Además los nodos pueden "pensar" (almacenar y procesar la información utilizando sus microcontroladores) y "hablar" (enviar y recibir información a través de un canal de comunicación, normalmente inalámbrico). Mediante el uso de estas capacidades, los nodos de una red de sensores pueden colaborar para adquirir información del mundo físico y proporcionarla a las entidades del mundo digital de forma directa o a través de un sistema "front-end" conocido como estación base."

Vid., LÓPEZ, J. y NÁJERA, P., *Los desafíos de seguridad en la Internet de los Objetos,* Revista SIC, vol.88, NICS Lab. Publications, Universidad de Málaga, 2010, p.69.

[45] *Vid.* RODRÍGUEZ LAÍNZ, J.L., *Internet de los objetos… op.cit.*

A modo ejemplar, los etiquetados electrónicos de determinados supermercados o grandes cadenas de distribución de moda, que no solo facilitan el cobro por caja o la salida de stocks de los almacenes, sin necesidad de lectura individualizada del código de barras de cada producto, sino que incluso transmiten la información en tiempo real a los ordenadores centrales de la cadena, sin intervención directa del ser humano, tomando incluso decisiones, en función de las existencias en almacenes, sobre reposición de determinadas mercancías, sistemas de vigilancia sanitaria …

Esta incipiente instauración de la IO no es el único ejemplo en el que la interconexión, por medio de las redes de comunicaciones electrónicas de determinados dispositivos, se realiza de forma automática permitiendo la gobernanza o mejora del rendimiento o capacidad de estos a través de diálogos automáticos. La permanente, que no constante, geolocalización de los terminales de telefonía móvil a través de las redes GSM, los sistemas de detección, análisis y actualización de software o ficheros de PC (que se activan con solo conectarlos a una red de comunicaciones electrónicas, sin necesidad de ejecutar un programa de navegación), la mejora de la calidad de la información facilitada por dispositivos de localización GPS (interactuantes con redes *WiFi*), o los sistemas de control o filtrado de paquetes para la mejora de la prestación de servicios de la sociedad de la información, son también una buena muestra de ejemplos pertinentes.

Analizando lo anterior desde un punto de vista jurídico, reviste especial interés el hecho de que estas conexiones[46] usan las redes conectivas electrónicas o Internet y es significativo, además, el dato de que los contenidos que, en muchas ocasiones, circulan por ellas se podrían considerar como información especialmente valiosa, capaz de hacer vulnerable el perfil, tanto comercial como íntimo de quienes están detrás de estos complejos sistemas electrónicos[47].

La utilización generalizada de este sistema plantea serios problemas y no solamente en lo referente a la categorización de los intercambios de información, como comunicaciones electrónicas dignas de idéntica protección que la brindada a una conversación telefónica, sino más en concreto la salvaguardia de la privacidad de los clientes, que podrían sentirse especialmente vulnerables ante un descontrolado flujo de información sobre consumo, del que podrían deducirse fácilmente sus hábitos de vida (estancias en el hogar o localización, adaptación al clima, derroche, valoración ponderada del número de personas que, de forma

[46] Por ejemplo, los sistemas de etiquetado inteligente suelen combinar el uso del espectro radioeléctrico en abierto con una canalización de la información a través de Internet.

[47] Como ejemplo, los contadores inteligentes, entendidos como dispositivos electrónicos que transmiten en tiempo real información, a través de las redes convencionales de comunicaciones electrónicas, sobre el consumo energético o de suministro de agua de cada vivienda o cliente individual; accesible tanto para el suministrador como para el propio cliente.

Este sistema de contadores ha encontrado su definitivo respaldo en la reciente Directiva 2012/27/UE, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, relativa a la eficiencia energética, por la que se modifican las Directivas 2007/127/CE y 2010/30/UE, y por la que se derogan las Directivas 2004/8/CE y 2006/32/CE.

habitual o esporádica, comparten vivienda con el usuario,…)[48]. Tanto es así, que la Directiva 2012/27/UE[49], del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, relativa a la eficiencia energética, siguiendo sin duda, los consejos del Supervisor Europeo de Protección de Datos[50], recoge en su artículo 9.2 una concreta obligación de asegurar "…la seguridad de los contadores inteligentes y la transmisión de datos, así como la privacidad de los clientes finales, de conformidad con la legislación pertinente de la Unión en materia de la protección de los datos y de la intimidad personal".

I.10.- Etiquetado en redes sociales

Aparte de los sistemas anteriores, hay muchos otros servicios que procesan datos de geolocalización que también pueden plantear problemas principalmente con la protección de datos así, por ejemplo, la tecnología de etiquetado geográfico específico vinculada a la denominada

[48] *Vid.*, RODRÍGUEZ LAÍNZ, J.L., *Internet de los objetos… op. cit.*

[49] Directiva 2012/27/UE, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, relativa a la eficiencia energética, por la que se modifican las Directivas 2007/127/CE y 2010/30/UE, y por la que se derogan las Directivas 2004/8/CE y 2006/32/CE.

[50] La Directiva fue precedida en este aspecto por la Recomendación de la Comisión de 9 de marzo de 2012, relativa a los preparativos para el despliegue de los sistemas de contador inteligente: http://www.edps.europa.eu (*Opinion of the European Data Protection Supervisor on the Comission Recommendation on preparations for the roll-out of Smart metering systems*) o su versión resumida en español publicada en el DOUE 2012/C 335, de 11 de noviembre de 2012.

Web 2.0 en la que los usuarios integran información con referencias geográficas en redes sociales[51], como *Facebook* o *Twitter*.

La Web 2.0 es una combinación de nuevas tecnologías y nuevas ideas que son el origen de una serie de nuevos servicios que con el tiempo se han convertido en elementos básicos de la sociedad.

Alrededor de muchas de las aplicaciones de Web 2.0 surgen nuevas comunidades de usuarios que interaccionan; es lo que sucede con las llamadas comunidades virtuales (por ejemplo, *Myspace*, *Tuenti*, *Facebook*, etc.), las cuales ofrecen, a su vez, servicios de geolocalización, de información, que nos permiten visionar y georreferenciar información en mapas o fotografías del territorio en el que se encuentre el usuario.

La evolución de la Web 1.0 a la Web 2.0 ha supuesto una nueva forma de definir de forma rápida y directa el entorno web que conocemos y utilizamos en la actualidad. Se ha pasado de un concepto estático basado en la lectura y/o revisión de contenidos a un concepto mucho más amplio y de carácter eminentemente dinámico, que se encuentra en continua evolución y enriquecimiento, por parte de los propios usuarios del sistema.

[51] Redes sociales online como *"plataforma de comunicación, a través de Internet, para que los usuarios generen un perfil con sus datos personales, facilitando la creación de redes en base a criterios comunes y permitiendo la conexión con otros usuarios y su interaccion"*.
ORTIZ LÓPEZ, P., *Redes sociales: funcionamiento y tratamiento de información personal,* en "Derecho y Redes Sociales", Editorial Civitas, Madrid, 2010, p.24.

El cambio conceptual ha sido profundo, partiendo de la idea inicial de Internet concebida como biblioteca, como almacén de múltiples documentos, en la que los usuarios realizaban consultas individualizadas o donde se publicaban contenidos de forma puntual, se ha alcanzado una nueva idea de la red entendida como un entorno interactivo y participativo utilizado por una pluralidad de usuarios en el marco de una Web Social Cooperativa, en la que cualquier usuario puede hacer pública su opinión y debatir con otros usuarios sobre servicios, productos, política, etc. Igualmente los usuarios pueden buscar y recibir información de interés, colaborar y crear conocimiento.

Se puede afirmar que la Web 2.0 es el resultado de la transición, desde aplicaciones tradicionales hacia aplicaciones que funcionan mediante el web enfocado al usuario final, poniendo especial énfasis en la colaboración online, en la interactividad y en la posibilidad de compartir contenidos entre usuarios, por ejemplo, su ubicación en el espacio[52]. Uno de los conceptos básicos de la Web 2.0[53] radica en que los usuarios no solamente consuman la información que aparece en la web, sino que a su vez la produzcan.

[52] NIETO MARTÍN. A., *Redes sociales en Internet y "Data Mining" en la prospección e investigación de comportamientos delictivos,* en "Derecho y redes sociales", Editorial Civitas, Madrid, 2010, p.219.

[53] La web 2.0 gira en torno a siete principios: 1)La web como plataforma, 2) Aprovechar la Inteligencia Colectiva, 3) Gestión de Base de Datos como competencia básica, 4) Fin del ciclo de actualizaciones de software, 5) Modelos de programación ligera, fácil plantillado, 6) Software no limitado a un solo dispositivo, y 7) Experiencias enriquecedoras del usuario.

Vid., WEB 2.0. Recuperado de: http://leonardoquinteros.blogspot.com.es/ (última consulta: 12 de enero de 2014).

Entre las herramientas que forman parte de esta Web 2.0, como ya hemos indicado, se encuentran redes sociales tales como *Facebook* y *Twitter*, donde existen numerosos peligros para la privacidad de sus usuarios. Unas veces, de forma voluntaria, estos comparten datos, fotografías, y ubicación geográfica en tiempo real etc.; mientras que otras, por desconocimiento, convierten, en datos de acceso público y general, informaciones privadas y de carácter personal.

En lo relativo a la geolocalización y siendo *Facebook*[54] el soporte que más información privada revela de sus usuarios, los "amigos" podrán conocer la ubicación del usuario por tres vías diferentes:

1.- Pestaña "Estoy aquí". Indica mediante texto la ubicación geográfica del usuario y la comparte públicamente con el resto de usuarios amigos.

2.- Pestaña de "Actualización de Estados". Cada vez que un usuario actualiza su estado, la red social facilita a los amigos de este primero, no una ubicación exacta, pero sí una aproximación del lugar donde se realizó la actualización de estado, indicando en un mensaje de texto referencias, tales como: "Hace 6 horas, cerca de Barcelona".

[54] FACEBOOK. Política de datos. Recuperado de: https://www.facebook.com/full_data_use_policy (última consulta: 22 de junio de 2015).

3.- *Facebook Messenger*. Cuando se envían mensajes privados entre dos usuarios de la red social, el remitente envía anexamente al mensaje que quiere trasmitir privadamente al receptor, la geolocalización del terminal móvil desde el que materializó la comunicación, en el momento de realizar la transmisión del mensaje.

Por su parte, en *Twitter*[55], tanto a través del ordenador como del terminal móvil, un usuario puede hacer pública la ubicación desde la cual está *tuiteando*. Si alguien pincha en un *tuit* de un usuario de la red, la ubicación que se muestra es muy precisa, tanto que se puede llegar a saber la calle y el número desde dónde el usuario está realizando esa acción.

Lo mismo ocurre con otras aplicaciones, como *Instagram* o *Google Maps*.

Instagram[56] permite el etiquetado de los lugares en los que se realizan las fotografías digitales de las que consta. Las geoetiquetas añaden información geográfica en los metadatos de las fotografías (en la mayoría de los casos sólo hacen referencia a las coordenadas, longitud y latitud del lugar donde fueron tomadas). Con independencia de lo anterior, lo más frecuente es que las fotografías que se toman desde la

[55] TWITTER. Política de datos. Recuperado de: https://about.twitter.com/es/what-is-twitter (última consulta: 30 de septiembre de 2014).

[56] INSTAGRAM. Política de privacidad. Recuperado de: https://help.instagram.com/155833707900388 (última consulta: 10 de junio de 2013).

cámara de un terminal móvil no incluyan esas geoetiquetas, a menos que se hayan configurado previamente[57].

En *Google Maps*[58], a través de la versión clásica del sistema, un usuario puede buscar sitios cercanos, así como obtener indicaciones hasta o desde la ubicación que ocupa en el momento de realizar la consulta de forma rápida (ejemplo "Como llegar") hasta el lugar de destino, relevando con ello de forma indirecta su ubicación geográfica.

I.11.- Geolocalización como comunicación

Por último, y, dentro de un proceso de comunicación, el usuario de un terminal móvil puede enviar a otro sus datos de posicionamiento geográfico (un ejemplo es el sistema *WhatsApp,* entre otros), datos que en este caso estarán protegidos, sin duda alguna, por el derecho al secreto de las comunicaciones, como se verá más adelante.

I.12.- Teledetección

[57] La función de geoetiquetado en la aplicación de las cámaras del *smartphone* requiere que el terminal disponga de GPS integrado.

[58] GOOGLE. Política de privacidad. Recuperado de: http://www.google.com/intl/es_es/policies/privacy/ (última consulta: 2 de abril de 2015).

El termino "teledetección" es una traducción del inglés *remote sensing*, y consiste en la adquisición de información a distancia, sin contacto directo con el objeto estudiado. Supone la captación de datos de la superficie terrestre y su posterior tratamiento con distintas finalidades, dentro del ámbito militar y civil. Estos datos son obtenidos desde el aire o desde sensores instalados en plataformas espaciales, en virtud de la interacción electromagnética existente entre la tierra y el sensor.

Son múltiples los usos que se dan a la teledetección, pero únicamente abordaremos el relativo a su aplicación al ámbito de la seguridad, que es el usado por las Fuerzas y Cuerpos de Seguridad del Estado en el esclarecimiento de ilícitos penales, tales como el control de las fronteras, el control medioambiental, el urbanismo y la ordenación del territorio, el control del tráfico marítimo, la protección de infraestructuras críticas, las tareas de seguridad ciudadana o incluso la captura de imágenes en alta resolución (de hasta 0,5 metros, capaces de detectar a una persona, aun en la más absoluta oscuridad o en condiciones climatológicas adversas mediante los sistemas Radar de Apertura Sintético o SAR)[59] necesarias para las unidades de investigación.

Las grandes limitaciones que rodean su uso conlleva actualmente su no empleo en el ámbito de la seguridad, así por ejemplo, a día de hoy, no se puede trabajar con estos medios en tiempo real, ya que antes de

[59] INSTITUTO GEOGRÁFICO NACIONAL. Recuperado de: http://www.ign.es/ign/layoutIn/faimgsatsatelite.do (última consulta: 16 de marzo de 2014).

obtener una imagen es necesario anticipar las coordenadas del punto a observar y, por el momento, el procesado de los datos capturados y la interpretación de los mismos es lenta.

II.- ESTUDIO ESPECIFICO DE DATOS DE GEOLOCALIZACIÓN DE ESTACIONES BASE, TRATADOS POR OPERADORES DE TELECOMUNICACIONES COMO RESULTADO DE LAS COMUNICACIONES MÓVILES O LA MENSAJERÍA INSTANTÁNEA

Como ya hemos visto de manera muy genérica en el punto anterior, los datos de geolocalización pueden ser obtenidos por las estaciones base como resultado de las comunicaciones móviles o de la mensajería instantánea realizadas desde un dispositivo móvil.

II.1.- Comunicaciones móviles

El concepto de comunicación móvil surge por la generalización del acceso radio[60], caracterizado porque el punto de acceso a la red varía en función de la posición que ocupe el usuario[61] en el sistema y que se logra por una red de transmisores y receptores (estaciones base) que conforman una estructura, compuesta por celdas, que abarca todo el territorio donde se presta servicio. Esta estructura permite la localización concreta del usuario dentro del sistema o *paging*, así como mantener la comunicación cuando el usuario se mueve de un punto a otro (o de una celda a otra), mecanismo denominado *hang over* o traspaso.

Este sistema de comunicaciones móviles está en plena evolución, de modo que el terminal ya no solo se usa para efectuar comunicaciones de voz, sino que, tras los llamados *smartphones* o teléfonos inteligentes, éstos ya permiten el intercambio de datos a través de conexión a la red de Internet (Internet móvil[62] o conexión móvil a Internet). Se intenta integrar todo tipo de servicios en una misma infraestructura, así como evitar que coexistan (como es el caso de España) distintos tipos de redes radio (2G, 3G, 4G…).

Este tipo de redes (*Next Generation Working* –NGN- o Red de Siguiente Generación) transportan la información mediante paquetes de

[60] "Radiocomunicación": *toda telecomunicación transmitida por medio de ondas radioeléctricas.* Anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

[61] "Usuario": *una persona física o jurídica que utiliza o solicita un servicio de comunicaciones electrónicas disponible para el público.* Anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

[62] Internet móvil entendido como el conjunto de servicios, aplicaciones y contenidos diseñados exclusivamente para usuarios móviles, independientemente de la plataforma móvil de acceso y la tecnología empleada.

datos encapsulados a través de Internet y son construidas a partir del Protocolo IP[63].

II.1.A.- Sistemas de comunicaciones móviles

Los sistemas de comunicaciones móviles permiten el intercambio de información entre terminales móviles y terminales fijos, o únicamente terminales móviles, a través de un medio de transmisión eléctrico con unas características de calidad determinadas.

Estos sistemas de comunicaciones móviles son de cobertura zonal; los terminales pueden estar en cualquier lugar dentro de dicha área de cobertura, habiendo evolucionado hacia un sistema de control y señalización sofisticado basado en técnicas digitales, lo que ha supuesto la mejora de la calidad de las comunicaciones, así como el desarrollo de nuevo servicios, por ejemplo, la transmisión de paquetes de datos.

El sistema de comunicaciones móviles está compuesto por:

- Subsistema de red: conjunto de equipos e instalaciones fijas, tales como controladores, nodos de conmutación y registros de usuarios y centros de control, operación y mantenimiento.

[63] Red *All-IP* para la tecnología 4G.

- Subsistema de acceso: conjunto de estaciones de radio, desplegadas por la zona de cobertura de la red móvil que permite el enlace de los terminales móviles entre sí o con terminales fijos, a través de dicha red. Podemos clasificar las estaciones de radio:

- Estaciones fijas (FS): son estaciones radioeléctricas no previstas para su utilización en movimiento.

- Estaciones móviles (MS): son estaciones radioeléctricas previstas para su utilización por el usuario en movimiento, dentro del área de cobertura; están compuestas por tres estaciones fijas (estaciones de base (BS), estaciones de control (CS) y estaciones repetidoras (RS)[64]).

II.1.B.- Evolución de los sistemas

La evolución se ha llevado a efecto a través de las siguientes etapas:

[64] Los terminales móviles se conectan a la red a través de la BS del subsistema de acceso. La conexión de la BS al subsistema de red se efectúa a través de línea metálica o fibra óptica, o mediante radioenlaces punto a punto. Las estaciones de radio de estos radioenlaces se llaman estaciones de control y en ellas, el tráfico es de tránsito.

Para la cobertura de entornos especiales donde no llega la estación base, se emplea a las estaciones repetidoras (RS), cuyo tráfico también es de tránsito, y que reciben la señal de la base y la irradian allí donde se encuentran las estaciones móviles (MS).

- Primera generación (1G): referida a los teléfonos móviles lanzados en los años 80 cuya tecnología era analógica, permitían únicamente llamadas de voz de baja calidad.

- Segunda generación (2G): surgió en los años 90, gracias a Instituto Europeo de Estándares de Comunicaciones, llegando mediante el estándar GSM, que pasó de la tecnología analógica a la digital, a permitir no solo el envío de voz (mejorado) sino también de datos (ejemplo de ello fueron los mensajes SMS).

- Generaciones intermedias (2,5G y 2,75G): fueron previas a la tercera generación; la 2,5G fue la más famosa por su estándar GPRS[65]. Introdujeron tecnologías basadas en la conmutación de paquetes de datos, lo que supuso una mejora en su transmisión, con velocidades mucho mayores que en la generación anterior, y la aparición de nuevos servicios: acceso a aplicaciones inalámbricas a través del WAP, envío de mensajes multimedia o MMS y acceso a servicios de comunicación por Internet (correo electrónico o páginas web).

[65] Las redes GPRS, a diferencia de las redes GSM, ocupan solo los recursos radio, cuando existe una necesidad de transmisión y, en el resto de momentos no. Los servicios GPRS están orientados a las aplicaciones que demandan una transmisión poco frecuente de pequeñas o grandes cantidades de datos.

- Tercera generación (3G): conocida por el estándar UMTS[66] con transmisión de datos a alta velocidad, a través de técnicas avanzadas de conmutación de circuitos y de paquetes, soportando tecnología IP, lo que la ha erigido en la Banda Ancha Móvil. La estructura de redes 3G está compuesta por la red de telecomunicaciones, que sustenta la transmisión de información entre los extremos de una conexión, y la red de gestión, que provee los medios para la facturación y tarificación de los abonados, el registro y definición de los perfiles del servicio, la gestión y seguridad en el manejo de sus datos, así como la operación de los elementos en red.

- Generaciones intermedias (3,5G y 3,75G): las cuales mejoran sensiblemente las velocidades de transmisión gracias al empleo de códigos que consiguen una mayor eficiencia espectral (HSDPA[67], HSUPA[68] o HSPA[69]). Dado que no requieren inversiones

[66] La arquitectura de red de UMTS mantiene los elementos de las redes GSM/GPRS con el fin de que el soporte de las redes UMTS sea lo más sencillo posible. La adopción de este servicio fue aprobada por el ETSI (*European Telecommunications Standards Institute*) y le son reservadas una serie de bandas de frecuencia para carga y descarga de datos. El problema de este servicio es el alcance que poseen sus antenas, ya que utilizan frecuencias en la banda de 2Ghz, lo que conlleva la necesidad de instalar más estaciones base a lo largo del territorio. Por el contrario, el número de usuarios admitidos es mayor y la potencia de los terminales menor, lo que supone el poder ofrecer más horas de servicio que para uno de tipo GSM.

Este método de transmisión emplea una técnica de acceso radio denominado CDMA (*Code Division Multiple Access*), donde todos los usuarios utilizan la misma frecuencia para la realización de la comunicación, pero con distinto código, y se necesita un buen control de la potencia para que la recepción de los usuarios sea similar.

Vid., LUQUE SOTO, R., "Uso policial y análisis forense de información…" *op.cit.*, p.31-32.

[67] Es la tecnología de transmisión de datos que optimiza el sistema UMTS. Es la evolución de la 3G de la tecnología móvil, conocida como 3,5G.

[68] Protocolo de acceso de datos para redes de telefonía móvil. Es una evolución del HSDPA.

significativas por parte de las operadoras, una vez instaladas las infraestructuras 3G, y debido al retraso que hubo en su lanzamiento, el despegue de estas generaciones ha coincidido con el auge de la 3G, por lo que muchos de los servicios ofrecidos han empleado estas tecnologías más avanzadas, sin que muchas veces el usuario tenga conocimiento de ellas.

- Antesala de la cuarta generación (3,9G): está liderada por el estándar LTE[70]; se basa en el empleo completo de tecnología de conmutación de paquetes sobre redes IPv6 y alcanza las velocidades de 100 Mbps o superiores, en caso de no estar en movimiento. El objetivo principal es proporcionar un acceso de radiofrecuencia de alto rendimiento, que permita altas velocidades de transmisión y recepción en dispositivos móviles y que pueda coexistir con HSPA y con los sistemas anteriores, permitiendo a las operadoras una rápida y sencilla migración hacia esta nueva tecnología. En este tipo de redes es posible el *handover*[71] entre redes móviles y redes inalámbricas de área local, manteniendo una calidad de servicio de punta a punta de alta seguridad para permitir ofrecer servicios de cualquier clase, en cualquier momento y con el mínimo coste posible.

[69] Es la combinación de varias tecnologías, como es la 3G y sus posteriores (HSDPA y HSUDPA). El HSPA+ hace referencia a su estándar evolucionado. Introducen la arquitectura IP.

[70] LTE o *Long Term Evolution*.

[71] Sistema utilizado en las comunicaciones móviles celulares con el objetivo de transferir el servicio de una base a otra, cuando la calidad del enlace es insuficiente.

La Unión Internacional de Telecomunicaciones estableció, en el año 2008, los requisitos para la cuarta generación, bajo el estándar *International Mobile Telecommunications-Advanced*[72]. Se dice que LTE es la generación 3,9G, ya que no cumple con estos requisitos y no puede ser considerada un estándar 4G[73].

- Cuarta generación (4G)[74]: básicamente se trata de una mejora de LTE para que cumpla las especificaciones de *IMT-Advance* y pueda ser considerado un sistema de cuarta generación. Actualmente, las redes 4G están optimizadas para un mundo en que las comunicaciones son todas IP; ofrece altas capacidades de transmisión con anchos de bandas de más de 100 Mhz (lo que permite realizar descargas de manera mucho más rápida) y realiza un mejor aprovechamiento del espectro radioeléctrico. En el momento presente, en España este sistema esta instaurado en la mayor parte de las capitales de provincia y continua extendiéndose. Tras ella surgirá la quinta generación o 5G.

---

[72] IMT-Advanced. Los principales requisitos para un estándar 4G son que está basado en un modelo de red "all-IP" que utilice únicamente la conmutación de paquetes, que alcance tasas de pico de 1Gbps en movilidad de baja velocidad (usuario quieto o a pie) y de 100 Mbps en movilidad de alta velocidad (trenes, coches, etc.) y, además, que alcance picos de eficiencia espectral de enlace de 15 bits/Hz y 6,75 bits/Hz en subida (es decir, que podamos descargar a 1Gbps con un ancho de banda de menos de 67 MHz). Incluye cuatro tipos de usuarios: estáticos, peatones, vehiculares y vehículos de alta velocidad.

Vid., LUQUE SOTO, R., "Uso policial y análisis forense de información…", *op.cit.*, p.32.

[73] LTE puede alcanzar velocidades de 300 Mbps y un ancho de banda de 20 MHz, en la interceptación de las nuevas formas de comunicación ofrecidas por los proveedores de servicios 4 0.

[74] En el Mobile World Congress celebrado en Barcelona, entre los días 27 de febrero a 1 de marzo de 2012, Telefónica ofreció una red móvil de cuarta generación en España o 4G para 2014/2015.

Esta secuencia de generaciones está caracterizada por el incremento sucesivo de capacidad de trasmisión (velocidades más altas de transmisión de datos) y por la aparición de contenidos de trasmisión más ricos.

II.1.C.- Interoperatividad entre redes GSM de telefonía móvil y estaciones BTS

A través de frecuencias reservadas a las redes de comunicaciones electrónicas[75], una parte del espectro radioeléctrico protegido es dedicado a los canales 2G, correspondientes a la tecnología GSM[76], por donde fluyen tanto las conversaciones telefónicas convencionales y los mensajes *SMS*, como toda una serie de diálogos automáticos de naturaleza técnica, entre terminal y estación BTS o antena de operadora, cuya función esencial es la de garantizar la efectividad del servicio, manteniendo permanentemente, que no constantemente, localizado al terminal.

Para tal fin, existen una serie de canales concretos entre los que se encuentra el llamado canal de control o RACH, cuyo cometido es comprobar periódicamente que el terminal sigue bajo la cobertura de una

[75] *Vid.,* RODRÍGUEZ LAÍNZ, J.L., *Internet de los objetos…*, *op.cit.*

[76] Directiva 87/372/CEE, de 25 de junio de 1987, relativa a las bandas de frecuencia a reservar para la introducción coordinada de comunicaciones móviles terrestres digitales, celulares públicas paneuropeas en la Comunidad —Directiva GSM— ; reformada por la Directiva 2009/114/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, y desarrollada por la Decisión 2009/766/EC de la Comisión, de 16 de octubre de 2009.

determinada BTS[77]. La BTS envía mensajes de confirmación del tipo información de señalización, por períodos regulares y, cuando el terminal pretende emitir una comunicación o está pendiente de recibir una llamada, el canal cambia automáticamente a lo que se denomina canal dedicado (única modalidad de canales bidireccionales que tiene la peculiaridad, no solo de transmitir las comunicaciones que efectuamos o recibimos, sino también de escrutar el espectro radioeléctrico, localizando otras BTS cercanas, pertenezcan o no a la misma operadora, a los efectos de tratar de garantizar la continuidad del servicio, ante el riesgo de pérdida o degradación de la cobertura).

Por otro lado, nos encontramos con los canales de difusión o BCCH, usados por las BTS para transmitir a los terminales telefónicos que se encuentran bajo su cobertura, consiguiendo así generar de los terminales, la contestación automática que hace vulnerable a dispositivos de captación el número IMSI del terminal receptor. Asimismo, se encuentran los ya mencionados canales dedicados, dentro de los cuales existe aquel que tiene por finalidad específica notificar el apagado o desconexión convencional (que no accidental) o la pérdida de energía del terminal. Así, cuando se producen situaciones de pérdida de cobertura,

[77] Cada estación base tiene un número de identificación único y está registrada con una ubicación específica. Tanto el operador de telecomunicaciones, como muchos dispositivos móviles, son capaces de utilizar las señales de casillas (estaciones base) solapadas para estimar la posición del dispositivo móvil con mayor precisión. Esta técnica es la denominada *triangulación*, de la que ya hemos hablado en apartados anteriores. Esta precisión puede incrementarse con la ayuda de parámetros como la intensidad de la señal recibida, la diferencia en el tiempo de llegada de la señal y el ángulo de entrada de la señal.

Vid., UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29, Dictamen 13/2011… *op. cit.*, p.4.

la BTS emite, durante 72 horas y, a períodos regulares, señales tendentes a tratar de recuperar la conexión con el terminal.

Ahondando aún más en lo que podríamos llamar la "vulnerabilidad del terminal", de entre todos los contenidos que comparten dichos terminales con las estaciones BTS se encuentran aquellos que permiten una localización geográfica bastante aproximada del terminal en un momento determinado[78], sin tener que intervenir o provocar una comunicación telefónica.

Se deduce de lo anterior que la interactuación entre terminales y estaciones BTS es muy fluida, y genera multitud de comunicaciones automáticas que trasmiten y reciben información especialmente valiosa, y no solamente de datos de localización o activación o desactivación de los terminales, sino incluso de datos relacionados con el mismo tránsito de las comunicaciones en las que sí tienen una participación directa los usuarios.

En el entorno de la Unión Europea, todas estas comunicaciones técnicas van encriptadas mediante un concreto algoritmo (en Europa, el A5/1), con la sola excepción de la activación del terminal. La vía de penetración por parte de terceros a esta información encriptada se realiza

[78] Si una BTS convencional divide su radio de acción en tres segmentos de 120º cada uno, a través de los llamados datos TA podemos conocer la distancia aproximada a la que se encuentra el terminal de la antena y ello, con un margen de error máximo de 550 metros, como segmentos en los que se subdivide el valor TA, hasta el límite máximo de su cobertura.

a través de falsas estaciones BTS, que dotadas de una mayor potencia que las convencionales, permiten la detección del terminal y establecen un diálogo con éste que, desprovisto de la encriptación, permite, a su vez, hacer permeable información de interés sobre el mismo. Esta será más detallada o profunda, en función de las capacidades de la herramienta empleada.

II.1.D.- Redes de nueva generación

La clara separación entre los mundos de la voz y los datos, en el ámbito de las telecomunicaciones, ha supuesto que los diferentes organismos de estandarización hayan sido también diferentes en la mayoría de los casos. Además, mientras que en el mundo de la voz las normas, en su mayor parte, son de obligado cumplimiento, en el mundo de los datos estas se desarrollaban por consenso entre los propios fabricantes y operadores, más como recomendaciones, que como normas preceptivas.

Para evitar este tipo de problemas, se ha buscado aglutinar en una única infraestructura de red las distintas alternativas existentes, de manera que se asegure un correcto funcionamiento de los servicios,

encontrando la solución en la evolución hacia un modelo NGN[79], basada en redes IP y al que se ha denominado *all-IP* o "Todo IP".

La Unión Internacional de Telecomunicaciones establece como elementos indispensables con que debe contar toda implementación de red que pretenda ser considerada como una red de nueva generación, los siguientes[80]:

- Ha de estar basada en conmutación de paquetes de datos.

- Necesaria separación de las funciones de control, transporte y servicios.

- Interfaces abiertas.

- Integración de servicios.

- Capacidades de banda ancha con calidad de servicio *end-to-end*.

- Integración con las redes actuales.

[79] NGN es un concepto para la definición y despliegue de redes, con una separación formal entre diferentes capas y planos con interfaces abiertos, que ofrece a los proveedores de servicios una plataforma sobre la que sea posible evolucionar paso a paso para crear, desplegar y gestionar servicios innovadores.

[80] La nueva tecnología 4G es, actualmente, la que más posibilidades tiene de consolidarse como la red móvil de nueva generación ya que cumple con dichas características.

- Movilidad.

- Acceso de los usuarios a distintos proveedores.

- Esquemas variados de identificación de usuarios.

- Servicios unificados y diseñados según la percepción del usuario.

- Convergencia de servicios Fijo-Móvil.

II.2.- Mensajería instantánea

Según un estudio elaborado, en julio del 2012, por Accenture y Ametic[81], los servicios de mensajería instantánea proporcionados por aplicaciones como *WhatsApp*, *Viber* o *Blackberry Messenger* igualan en penetración al correo electrónico, situándose en el 70%. El informe resume que *"la frecuencia de uso del email decrece en 2012 en favor de la mensajería instantánea"*, lo que indica que este servicio se ha convertido en *"el estándar de comunicación móvil"*.

[81] ACCENTURE, "Always on. Always connected. Liderando la creación de un ecosistema digital sostenible", Estudio de 23 de julio de 2012, elaborado por Accenture y Ametic. Recuperado de: http://www.accenture.com/es-es/Pages/always-on-always-connected-study-acn-ametic-2012.aspx (última consulta: 23 de enero de 2015).

El surgimiento de la mensajería instantánea es relativamente nuevo y se trata de una evolución de los servicios *chat* para el ordenador que se llevan usando desde hace años. *Google Talk*, *AIM*, *Yahoo Messenger*, *Microsoft Messenger* son, entre otros, los precursores de esta tendencia. La principal razón del éxito de esta nueva forma de comunicación es la proliferación de los actuales teléfonos móviles inteligentes o *smartphones*. En la mayoría de los casos, estos requieren una conexión a Internet, lo que nos da acceso a múltiples aplicaciones y utilidades que hasta ahora habían estado reservadas al sector informático de escritorio. Además, el coste gratuito (salvo el consumo de datos en sí generados, al realizar esta operación) y las opciones añadidas (acciones como enviar un mensaje automáticamente a un grupo de personas, mantener conversaciones con pluralidad de personas al mismo tiempo y la ausencia de limitación en la longitud del mensaje), están desbancado el uso de la mensajería tradicional.

II.2.A.- Concepto y características de la mensajería instantánea

La mensajería instantánea (IM) es un servicio de software de comunicación que utiliza el protocolo TCP/IP, permitiendo la comunicación en línea entre dos o más personas conectadas a Internet u otras redes; ofrece, además de la posibilidad de enviar y recibir mensajes

instantáneos, distintas opciones de aplicación, entre las que se encuentran los servicios de presencia (o capacidad de reconocer si un usuario de nuestra lista se encuentra en línea o no), el de asignar un icono a sus participantes, el de emitir una señal sonora y la transmisión de archivos, entre otros, sin olvidarnos de que las últimas tendencias van encaminadas a la inclusión generalizada de servicios como telefonía IP y videoconferencias.

Más concretamente, el servicio IM permite una comunicación en tiempo real entre dos o más miembros conocidos (diferencia fundamental con los chats tradicionales). Los usuarios están conectados permanentemente a su red IM desde sus teléfonos móviles, de manera que una de las utilidades que ofrece es la de conocer el estado de los demás usuarios de su lista de contactos.

Se destaca asimismo por la seguridad en la información que está siendo enviada a través del sistema, y ello debido al modo de transmisión de los datos que, de manera resumida, es el siguiente: el teléfono se conecta a un servidor para enviar un mensaje a través de una aplicación, y es este servidor quién se encarga de validar al destinatario mediante una contraseña antes de presentar el mensaje en el aplicativo del cliente de destino. Si el destinatario no se encuentra en ese momento disponible, el servidor guarda ese mensaje en una cola de salida, de manera que cuando el destinatario se conecte, recibirá instantáneamente el mensaje en su aplicación móvil.

Destacable también es que el servicio IM soporta el *Modo Background*, el cual permite que la aplicación quede en un segundo plano, utilizando lo mínimo de batería hasta que se reciba una alerta o un usuario inicie una conversación IM.

II.2.B.- Infraestructura de la mensajería instantánea

Los primeros modelos de IM, como *AOL Instant Messenger* o *MSN Messenger*, usaban la arquitectura cliente-servidor. Sin embargo, debido al incremento del número de clientes, el coste de los servicios y la mala calidad de las comunicaciones, se cambió al modelo *Peer to Peer* (P2P)[82]. Basándose en la estructura *Peer to Peer* (P2P) *híbrida*, solución que aprovecha las ventajas de las arquitecturas cliente-servidor y P2P, podemos decir que la mensajería instantánea opera utilizando una infraestructura formada por los siguientes componentes:

- Los clientes o nodos, que representan las aplicaciones software que los usuarios instalan en sus dispositivos.

[82] Las redes *peer to peer* son redes descentralizadas y distribuidas, en las que las aplicaciones pueden comunicarse entre sí intercambiando información sin la intervención de un servidor central; es decir, es una red donde no existen clientes y servidores fijos, sino una serie de nodos que se comportan a su vez como clientes y servidores de los demás. La clave fundamental del *peer to peer* es que los nodos son tratados de "igual a igual", como indica su terminología anglosajona.

- Los servidores, que no son más que los proveedores de servicios (IP accesible), que actúan de nexo entre los clientes, empleando los servidores públicos.

- La infraestructura de redes, que es el medio subyacente por el cual se establece la comunicación entre cliente/servidor en un sistema IM. En el caso que tratamos se trata de la red de Internet móvil.

II.2.C.- Funcionamiento

Como ya se ha expuesto, la mensajería instantánea está basada en el modelo de arquitectura P2P híbrida, que combina las soluciones cliente/servidor y P2P.

Para el envío y entrega de mensajes en tiempo real se basa en la arquitectura cliente servidor. El cliente se instala en el dispositivo del usuario final y mediante la interface del software de la aplicación, se establece la comunicación con otros miembros. El servidor, a su vez, tiene varias tareas de relevante importancia:

- Administrar y regular absolutamente todas y cada una de las comunicaciones de los usuarios.

- Mantener activos todos los servicios.

- Proporcionar mecanismos de seguridad por medio de la autenticación de usuarios.

- Verificar el estado de los mismos durante el tiempo que estos se encuentren activos en la comunicación.

a) Establecimiento de la conexión e identificación del cliente

Cuando un cliente A ingresa al sistema de IM, se conecta al servidor central S a través de un protocolo propietario para la comunicación, que varía dependiendo del software utilizado. Este servidor central deberá verificar la identidad de A y registrarlo para poder establecer la apertura de una nueva sesión. Posteriormente, el cliente A proporcionará la información de conexión al servidor (su dirección IP y el número de puerto asignado al cliente), siendo dicha información almacenada temporalmente en el servidor conjuntamente con una lista de contactos, por ejemplo B, C y D, cuyos integrantes serán verificados para comprobar a su vez si estos también se encuentran ya registrados[83].

Si esto fuera así, el servidor enviará un mensaje *multicast*[84] al subconjunto de potenciales clientes que figuren identificados

[83] TYSON, J., *How Instant Messaging Works*. Recuperado de: http://vclass.mgt.psu.ac.th/~parinya/MISMBA2004/sectionII/hardware-howstuffworks/HSW-communication/instant-messaging.pdf

[84] Un mensaje multicast es *"[…] aquella técnica que permite que copias de un solo paquete se transfieran a un subconjunto seleccionado de todos los posibles destinos".*

notificándoles que el cliente A se encuentra activo. Por supuesto, a su vez, el cliente A recibirá la respuesta del servidor con la información de quiénes se encuentran registrados y activados en el sistema de IM.

b) Intercambio de mensajes

Una vez establecida la conexión, podemos seleccionar un integrante de la lista y enviarle un mensaje, por ejemplo, al usuario B, escribiéndolo en la ventana de mensaje. El cliente A obtendrá la dirección IP y el puerto de acceso del usuario B, por lo que el mensaje será directamente enviado a ese host[85]. Una vez que el cliente C reciba el mensaje de A, puede responderlo al instante.

La recepción y el envío de mensajes se realizan a través de unos protocolos que trataremos más adelante.

c) Cierre de la conexión

Si el usuario A desea terminar la comunicación, se cierra la ventana de mensajes y pasa al estado desactivado y sale del software de IM. El cliente de IM envía un mensaje al servidor central S para notificarle que ha concluido la sesión. Este servidor central enviará un

Vid., DOUGLAS E. COMER, *Redes Globales de Información con Internet y TCP/IP*. Recuperado de: http://librosgratis.net/book/redes-globales-de-informacion-con-internet-y-tcp-ip-ra edicion-douglas-e-comer_1596.html (última consulta: 11 diciembre 2015).

[85] *Host* o dispositivo que funciona como punto de inicio y final de las transferencias de datos por medio de una dirección IP que tienen asignada dentro de la red.

mensaje multicast a todos los clientes de la lista de contactos para informarles de que el usuario A ha salido de la sesión.

II.2.D.- Protocolos de la mensajería instantánea

Un protocolo de IM define la interacción entre los servicios de la IM, los remitentes de los mensajes y la carpeta de correo entrante instantáneo.

En la actualidad no existe claramente un protocolo uniforme para todos los sistemas de IM, sino que cada uno de ellos implementa su propio esquema de reglas y normas de funcionamiento, lo que es una considerable desventaja. Además, algunos de ellos son propietarios y, por tal motivo, no ofrecen documentación ni dan acceso a sus fuentes.

Dentro de las iniciativas más importantes que se han propuesto para la normalización y estandarización del servicio de IM, figuran los protocolos de la IETF[86].

[86] IETF o *The Internet Engineering Task Force* es una comunidad internacional abierta de diseñadores de redes, operadores, vendedores e investigadores preocupados por la evolución de la arquitectura de Internet y el buen funcionamiento de Internet, nacida el 16 de enero de 1986 con financiación del gobierno de los Estados Unidos. Esta organizada en grupos de trabajo, cada uno dedicado a un tema específico, tras cuya investigación el grupo se disuelve.
Vid., IETF. Recuperado de: http://www.ietf.org/ (última consulta: 9 de junio de 2016).

a) SIP

Es un protocolo de control y señalización usado mayoritariamente en los sistemas de telefonía IP, que fue desarrollado por un grupo de trabajo de IETF en el año 1999 (RFC 3261). Dicho protocolo permite crear, modificar y finalizar sesiones multimedia con uno o más participantes y sus mayores ventajas recaen en su simplicidad y consistencia. La sintaxis de sus operaciones se asemeja a las de HTML y SMTP, los protocolos utilizados en los servicio de páginas web y de distribución de *emails,* respectivamente. Esta similitud es natural, ya que SIP fue diseñada para que la telefonía se convierta un servicio más en Internet.

b) OSCAR

Es el protocolo oficial del programa de mensajería instantánea de AOL, AIM. Es un desarrollo propietario y no ofrece ninguna documentación ni dan acceso a sus fuentes. Por esto, muchos diseñadores de programa soporte para múltiples plataformas de mensajería, han tenido que recurrir a la ingeniería inversa para conocer su forma de actuar y adaptar sus programas para hacerlos compatibles con AIM.

Oscar funciona en tres pasos: primero realiza la autentificación del usuario, después entra en funcionamiento el sistema de envío y recepción

de datos (BOS) y finalmente, el navegador del Chat crea la sala de charlas.

c) WMPP

Surgido en 1998, se trata de la especificación base de *Jabber* y es conocido como el primer estándar de carácter abierto. Fue tomado como protocolo por el grupo Open Source en 1999, donde ha ido creciendo y evolucionando hasta la actualidad.

Este protocolo establece una plataforma para el intercambio de datos XML y puede ser usado entre las aplicaciones de Internet para mensajería instantánea. Posee unas características muy significativas que le proporcionan adaptabilidad y sencillez. Entre otras de sus posibilidades de uso, ofrece servicios, tales como, un directorio de usuario, salas de charla pública o puentes a otras mensajerías como el *email* o el *MSN*.

Este es el protocolo que eligió *Google Talk*, *Facebook Messenger* y el servicio de mensajería de *Tuenti*.

II.2.E.- Clientes móviles de mensajería instantánea

Los clientes móviles son la solución que ofrecen diferentes empresas proveedoras para que sus suscriptores puedan acceder a la

mensajería instantánea desde sus teléfonos móviles. Ante el auge del uso de estos servicios por los usuarios, cada vez son más las que crean nuevas soluciones, desarrollando aplicaciones de mensajería instantánea de valor añadido para convivir con los servicios de mensajería instantánea tradicionales como *Yahoo! Messenger*, ICQ, AIM, *Windows Live Messenger*, etc. Tal es la revolución que se está produciendo, que muchos de los servicios tradicionales se han visto obligados a ofrecer las versiones móviles de sus aplicaciones.

Los más conocidos y empleados actualmente son:

a) WhatsApp

Ilustración 3: WhatsApp

WhatsApp, comprado en el 2014 por *FaceBook*, es una aplicación de mensajería multiplataforma que permite enviar y recibir mensajes sin pagar por SMS, así como imágenes, video y audio. Está disponible para iPhone, BlackBerry, Windows Phone, Android y Nokia[87].

[87] WhatsApp. Recuperado de: http://www.whatsapp.com/ (última consulta: 15 de mayo de 2015).

Es considerada por muchos como la mejor aplicación de mensajería instantánea.

WhatsApp ofrece muchas posibilidades en relación con los datos de geolocalización. No solo podemos insertar, dentro de nuestro mensaje escrito, información relativa a dónde nos encontramos, sino que permite al usuario enviar, como mensaje inserto en la comunicación, un archivo con la ubicación de la persona en un plano detallado, con un escaso margen de error, siempre y cuando se haya permitido a la aplicación acceder al sistema GPS del teléfono móvil. Asimismo se podría remitir un audio al interlocutor con el que se esté manteniendo una conversación donde se informe del posicionamiento geográfico.

b) Blackberry Messenger

Ilustración 4: Blackberry Messenger

Aplicación de mensajería instantánea que, no solo permite una conversación a través de mensajes de texto, sino también acceder a un

chat de BBM Voice para poder hablar con el resto de usuarios identificados de manera gratuita a través del uso de una red *WiFi*[88].

Research In Motion Ltd (RIM) revolucionó el mundo de los terminales móviles con la aparición de la BlackBerry en 1999. De hecho, actualmente dicha compañía opera en todo el mundo bajo el nombre de BlackBerry.

Los servicios que presta BlackBerry consisten en:

- Los terminales de la marca BlackBerry, los cuales poseen un identificador único que individualiza cada terminal y, además, permite que los datos que se transmiten se cifren (lo cual, sin duda, supone una comunicación más segura).

- Un centro de comunicaciones, denominado NOC[89], que se ocupa de enlazar los terminales. Solamente existen tres en toda la geografía del planeta; están situados en Canadá (dando cobertura a América), en Estados Unidos (dando cobertura a Asia) y en Gran Bretaña (dando cobertura a Europa, África y Oriente Medio).

- Una red propia de comunicaciones por donde se dirige el tráfico de sus servicios.

[88] BLACKBERRY MESSENGER. Recuperado de: http://appworld.blackberry.com/webstore/content/3729/?lang=es&countrycode=ES (última consulta: 23 de abril de 2014).

[89] Network Operating Center.

- Unos servidores que almacenan los identificadores únicos de los terminales y las direcciones de correos a las que están asociados. BlackBerry ofrece dos servidores:

- BES[90], es un servicio para las empresas que permite al usuario acceder a una Intranet corporativa. La comunicación se establece a través de Internet con los servidores NOC por un puerto conocido. Cuando se conecta, el servidor BES avisa a todos los dispositivos que tienen asociados. La comunicación siempre se inicia desde el BES, nunca desde fuera, hecho que dota a este servicio de gran seguridad.

- BIS[91], es un servicio desarrollado principalmente para usuarios particulares. En este caso, el terminal Blackberry se registra en el servidor de un operador de red, que será el que le da acceso a los diferentes servicios a través de la infraestructura RIM.

El NOC de BlackBerry es un componente clave. Cuando se instala por primera vez, se le asigna una dirección única llamada *Server Relay Protocol IP* (SRP IP) para que pueda ser identificado, utilizándola cada vez que un dispositivo Blackberry se conecta al NOC. De este modo, el NOC reconoce el BES y el terminal asociado al mismo, lo que permite la

[90] Blackberry Enterprise Server.
[91] Blackberry Internet Service.

comunicación entre ambos. Por tanto, el NOC es el punto donde los terminales y los servidores BES se encuentran y comunican. Se ocupa de manejar las conexiones individuales de cada Blackberry y redirige los datos que van dirigidos a un móvil.

Las comunicaciones que se producen entre el dispositivo y el servidor BES están aseguradas por el empleo de la tecnología de encriptado AES 256, considerada inviolable, y es aquí donde surgen los primeros problemas para la interceptación y análisis de las conversaciones por las Fuerzas y Cuerpos de Seguridad del Estado, a lo que se ha de añadir que todo el tráfico de datos (correo, navegación, mensajes instantáneos, etc.) de los terminales Blackberry pasa por uno de los tres servidores nombrados anteriormente, los cuales están fuera de la jurisdicción española.

La inviolabilidad de las comunicaciones Blackberry son bien conocidas por todo el mundo. Los criminales y delincuentes han optado por emplear, como medio de comunicación, soluciones como las que se han descrito, lo que dificulta la intervención de las mismas y, en definitiva, retrasa la investigación de las actividades delictivas.

c) Google Hangouts

Ilustración 5: Google Hangouts

Es la versión que sustituye a *Google Talk*, que ha evolucionado desde la mensajería instantánea y VoIP[92], de protocolo XMPP, hasta la creación de una plataforma asociada a una cuenta de Gmail (*email*) con el objeto de realizar conferencias de video, audio o intercambio de mensajes, donde lógicamente las posibilidades al respecto del contenido de la comunicación son infinitas, incluyendo por tanto los datos de geolocalización de los interlocutores[93].

Como plataforma exclusivamente de mensajería tenemos a *Google Allo*[94].

[92] Con estas siglas VoIP se conoce la *voz sobre IP*, una tecnología que combina distintos programas y periféricos que permiten usar la conexión a la red como si se tratase de una línea telefónica convencional. El sistema digitaliza la voz del usuario y la envía en paquetes mediante un protocolo de Internet, en vez de hacerlo a través de la red telefónica. La principal ventaja del VoIP es que el servicio es gratis entre usuarios que usen el mismo sistema, ya que no hay que pagar a las compañías telefónicas. Entre las desventajas que indican sus detractores se encuentra la calidad de la transmisión, que en ocasiones es inferior a la telefónica, pues los paquetes de datos de voz pueden ser recibidos de forma defectuosa.

[93] GOOGLE HANGOUTS, anteriormente conocido como *Google Talk*. Recuperado de: https://www.google.es/talk/intl/es/ (última consulta: 23 de mayo de 2016).

[94] GOOGLE ALLO. Recuperado de: https://allo.google.com (última consulta: 23 de mayo de 2016).

d) Viber

Ilustración 6: Viber

Permite realizar llamadas VoIP de bastante buena calidad a otros usuarios que también tengan descargada la aplicación en sus dispositivos, así como enviar mensajes; funciona, en este caso, de manera muy similar a *WhatsApp*[95].

Esta aplicación está disponible para iOS, Android, Windows Phone, Nokia, Blackberry y Bada.

e) Tango

Ilustración 7: Tango

Valido para iOS y Android, y permite realizar llamadas VoIP entre los usuarios de esta aplicación, el envío de mensajes, así como archivos

[95] VIBER. Recuperado de: http://www.viber.com/ (última consulta: 4 de mayo de 2016).

de audio, video o imágenes, con posibilidad de remisión de la ubicación del interlocutor. Es de características similares a Viber[96].

f) Pidgin

Ilustración 8: Pidgin

Anteriormente llamado Gaim, es un cliente de mensajería instantánea multiplataforma capaz de conectarse a múltiples redes (multiprotocolo) y cuentas de manera simultánea. Muestra en diferentes pestañas las diversas conversaciones que se mantienen y permite el envío de archivos, avisando asimismo cuando un contacto se conecta o se desconecta de la red[97].

Lo realmente novedoso es que sus mensajes son cifrados utilizando plugins (Pidgin-Encryption y OTR-Plugin).

[96] TANGO. Recuperado de: http://www.tango.me/ (última consulta: 2 de mayo de 2016).

[97] PIDGIN. Recuperado de: http://www.pidgin.im/(última consulta: 28 de octubre de 2016).

g) Nimbuzz Messenger

Ilustración 9: Nimbuzz Messenger

Combina el servicio de llamadas VoIP, la mensajería instantánea y la geopresencia[98].

Es compatible con Windows Live, Yahoo! Messenger, Facebook, Google Hangouts, AIM, MySpace, Hyves e ICQ.

h) *ChatON*

Ilustración 10: ChatON

Es la aplicación multiplataforma de mensajería gratuita de la compañía Samsung, que cuenta con versiones para Android, iOS y Blackberry OS. Además de enviar mensajes de texto, permite remitir

[98] *NIMBUZZ MESSENGER*. Recuperado de: http://www.nimbuzz.com/en/ (última consulta: 22 de noviembre de 2015).

archivos de audio y video así como mensajes animados a nuestros contactos[99].

i) *Line*

Ilustración 11: Line

Es una aplicación para terminales móviles, así como para PCs, que permite las llamadas VoIP, así como la mensajería instantánea donde se incluye la posibilidad de remitir, tanto archivos de audio y video como mensajes animados o *stickers*[100].

j*) GroupMe*

Ilustración 12: GroupMe

[99] SAMSUNG. ChatON. Recuperado de: http://www.samsung.com/es/article/que-es-chaton (última consulta: 12 de mayo de 2016).

[100] LINE. Recuperado de: http://line.naver.jp/en/ (última consulta: 11 de noviembre de 2015).

Es un servicio de mensajería instantánea comprado por Skype, perteneciente a Microsoft. Es una aplicación para terminales móviles, así como para PCs, que permite los mensajes grupales y los directos entre sus usuarios, así como la geolocalización. Disponible para Android, iOS, Windows Phone y Blackberry[101].

k) Paltalk

Ilustración 13: Paltalk

Es una de las aplicaciones más completas y potentes del mercado, pero ello supone el inconveniente de la mayor complejidad en su uso. Permite llamadas de voz, de video con hasta 10 usuarios, video chats, video rooms, y, por supuesto, mensajes instantáneos[102].

Ofrece varias versiones de las cuales solo la denominada Basic es gratuita.

[101] GroupMe. Recuperado de: https://groupme.com/ (última consulta: 12 de junio de 2016).

[102] PALTALK. Recuperado de: http://es.paltalk.com/ (última consulta: 7 de febrero de 2016).

Su característica principal es la posesión de salas de conversación con variedad de contenido (adulto, karaoke y otros) que pueden ser creadas por los propios usuarios. En estas salas, los usuarios pueden enviar mensajes de conocimiento público o de forma privada a algún usuario en especial.

l) IM+

Ilustración 14: IM+

Servicio desarrollado por Apple que, además de mensajes instantáneos, permite la transferencia de archivos y compartir la localización con otros usuarios. Permite, igualmente, hablar con los usuarios de la mensajería instantánea y, al tiempo, consultar las redes sociales. Soporta Windows Live, Facebook, Yahoo!, Google Talk, AOL, ICQ, VKondake, Yandex, MySpace, Jabber y Twitter[103].

m) Telegram

[103] IM+. Recuperado de: https://plus.im/ (última consulta: 11 de julio de 2016).

Ilustración 15: Telegram

Surgió en el 2013 y tiene millones de usuarios. Tiene fama de ser la plataforma más segura en cuanto a preservar la privacidad de los usuarios. Es la gran competidora de *WhatsApp*[104].

n) Spotbros

Ilustración 16: Spotbros

Esta aplicación, de origen español, nacida en el 2012, permite el envío de mensajes instantáneos con algunos extras como el poder participar en chat públicos o privados[105]. Concretamente destaca por dos funcionalidades:

[104] TELEGRAM. Recuperado de: https://telegram.org (última consulta: 6 de mayo de 2015).

[105] SPOTBROS. Recuperado de: http://www.spotbros.com/ (última consulta: 6 de noviembre de 2015).

- El *shout*: mensajes que puedes enviar a otros usuarios localizados en un radio de 1,5 km para pedir o dar información, solicitar ayuda, avisar sobre algo...

- El *spot:* grupo público geolocalizado, sin límite de miembros, donde se comparte información sobre un tema en particular.

Incluye otras aplicaciones útiles, denominadas SBApps, como la programación de televisión, la cartelera, un traductor o conocer el tráfico…

Con cierto parecido a las redes sociales, especialmente a Facebook, también permite poner un determinado estado, comentar los de otros y cambiar la foto de perfil en un "muro" que se muestra al resto de contactos.

Aparte de lo anterior, se puede decir que su característica más importante es la seguridad, ya que cifra todas las conversaciones de los usuarios con el algoritmo AES 256 (el mismo que emplea Blackberry o el gobierno de los Estados Unidos) y cada 30 días se elimina toda la información almacenada en los servidores de los usuarios.

II.3.- Aplicaciones informáticas en dispositivos electrónicos

Como ya se avanzó de manera genérica en el punto anterior, en prácticamente todos los terminales móviles de comunicaciones existen estas aplicaciones de mensajería instantánea y otras aplicaciones informáticas que pueden ser ejecutadas por el usuario, empleando conectividad IP y tráfico de datos y que utilizan datos relativos a la localización del terminal para prestar multitud de servicios al usuario[106]. Actualmente la mayoría de los dispositivos cuentan con tecnología GPS, lo que les lleva a poder calcular su posición con una gran precisión y con márgenes de error menores a 15 metros.

Todas estas aplicaciones generan un gran número de datos de localización, normalmente en coordenadas GPS, que fluyen a través del tráfico de datos IP que envía y recibe el usuario registrado en la red celular.

Como se verá en el próximo capítulo, estos datos pueden ser accesibles a través de intervenciones legales de las comunicaciones o acceso a los datos de tráfico dentro de un procedimiento judicial, o mediante su captación directa de la interfaz radio en el aire, mediante el empleo de medios tácticos de interceptación.

[106] Un ejemplo de ello es la aplicación de Apple para Iphone, Ipad y Ipod llamada "Buscar mi IPhone", la cual, entre otros servicios, posiciona cualquiera de los dispositivos del usuario en tiempo real pudiendo averiguar, si se diera el caso, incluso la trayectoria de su movimiento.

Vid., APPLE. ICloud. Aplicación "Buscar mi IPhone". Recuperado de: http://www.apple.com/es/icloud/find-my-iphone.html (última consulta: 2 de abril de 2015).

III.- CONCEPTO Y REGULACIÓN JURÍDICA. ESPECIAL REFERENCIA A LA DECLARACION DE INVALIDEZ DE LA DIRECTIVA 2006/24/CE POR LA SENTENCIA DEL TJUE, GRAN SALA, DE 8 DE ABRIL DE 2014

Tras presentar una visión general de la tipología de los datos de geolocalización en el ámbito tecnológico, debemos hacer la correspondencia con la normativa existente que regula algunos aspectos de dicha información.

III.1.- Marco jurídico europeo

Dentro del marco europeo, podríamos definir los datos de geolocalización haciendo uso del concepto de "datos de localización" fijado por la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[107], en la cual queda identificado en su artículo 2.c como "*Cualquier dato tratado en una red de comunicaciones*

[107] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas -*Directiva sobre la privacidad y las comunicaciones electrónicas*-, DOUE, núm. 201, de 31 de julio de 2002.

electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público". Posteriormente se elaboró la Directiva 2006/24/CE de 15 de marzo, del Parlamento Europeo y del Consejo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE[108], norma que no afecta a la definición anterior[109].

Continuando con la Directiva 2002/58/CE, esta aclara en su considerando 14 que tales datos "pueden referirse a la latitud, la longitud y la altitud del equipo terminal del usuario, a la dirección de la marcha, al nivel de precisión de la información de la localización, a la identificación de la célula de red en la que está localizado el equipo terminal en un determinado momento a la hora en que la información de localización ha sido registrada".

Por su parte, el artículo 9 de esta Directiva distingue entre los datos de localización como datos de tráfico o "datos de cobertura" y aquellos que no lo son o "los datos de localización distintos de los de tráfico":

[108] Directiva 2006/24/CE, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, DOUE, núm. 105, de 13 de abril de 2006.

[109] Esta Directiva 2006/24/CE ha sido recientemente anulada por la STJUE de 8 de abril de 2014 debido a la escasa definición en la norma de las cautelas y garantías jurídicas precisas y claras que exige la inmisión en el derecho a la protección de datos personales.

a) Los "datos de cobertura" son los tratados por los operadores de comunicaciones a fin de ubicar, en el espectro radioeléctrico, los terminales de telefonía móvil para poder hacer efectiva la eventual comunicación, de modo que este tratamiento es previo, simultáneo y posterior al hecho mismo de la comunicación, por lo que, solo cuando la ubicación geográfica que señalan tales datos se presenta accesoriamente a una comunicación en curso, puede calificarse de datos de tráfico.

Respecto a estos "datos de cobertura" como datos de tráfico, por encontrarse integrados en un proceso comunicativo, cada operador genera y puede disponer, con distintas finalidades, de una base de datos permanentemente actualizada o CDR (*Call Data Record)*, donde se registra la referencia de cada una de las comunicaciones, incluidas las infructuosas. Estos registros contienen el número de teléfono de origen y destino, IMEI de los terminales de origen y destino, tiempo y tipo de servicio, conservando las coordenadas de situación geográfica de las estaciones base (BTS) origen y destino de la comunicación.

b) Respecto de "los datos de localización distintos de los de tráfico", podemos diferenciar dos categorías:

- Datos de cobertura sin comunicación[110], que proporcionan la localización del terminal independientemente de que exista comunicación o no, debido a que siempre que un terminal móvil se conecta a la red GSM, su localización geográfica queda almacenada en un registro de la compañía operadora (HLR o *Home Location Register*), posición que, como ya se ha explicado en el apartado anterior, se irá actualizando permanentemente sin que el usuario sea consciente y con la única finalidad de que este siga conectado a la red.

- Datos de localización como servicios de valor añadido, como son los de GPS o similares. Son un conjunto de información necesaria para que los operadores proporcionen a sus abonados los llamados "servicios basados en la localización" (LBS o *Location Based* Services), respecto de los cuales se exige que solo puedan ser tratados en el caso de que sean anónimos o con el consentimiento del usuario. Es necesario, si estos datos no han sido determinados con carácter anónimo, que el usuario sea informado de su recopilación, tratamiento, finalidad y duración, caracteres del mismo y posible cesión (en el sentido de transmisión a un tercero a efectos de la prestación del servicio

[110] También denominados por PÉREZ GIL como "datos *stand by*" o datos que hipotéticamente posibilitarían una comunicación si se iniciasen las actuaciones conducentes a ella, pero que en realidad no satisfacen esa función.

Vid., PÉREZ GIL, J., *El nuevo papel de la telefonía móvil en el proceso penal…*, *op.cit.*, p. 153.

con valor añadido), ya que en caso contrario, la prestadora no estará habilitada para ello[111].

Las diferencias legales y técnicas entre las diversas disposiciones nacionales sobre la conservación de datos con fines de prevención, investigación, detección y enjuiciamiento de delitos creaban obstáculos en el mercado interior de las comunicaciones electrónicas. Como consecuencia, los prestadores de servicios debían cumplir requisitos diferentes en cuanto a los tipos de datos de tráfico y de localización que deben conservarse, así como en cuanto a las condiciones y los períodos de conservación. Esto se hizo patente a la luz de esta Directiva 2002/58/CE del Parlamento Europea y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (norma que sustituyó a la Directiva 97/66/CE) que no era aplicable a las actividades del Estado en materia penal de conformidad con su artículo 1.

Hubo que esperar a las **conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002** para que se diera a esta materia, un ápice de la importancia merecida. Así se destacó entonces que, a causa del crecimiento significativo de las posibilidades de las comunicaciones electrónicas, los datos relativos al uso de las mismas eran particularmente importantes y, por tanto, una herramienta valiosa

[111] Artículo 48.2 de la Ley 9/2014, de 9 Mayo, General de Telecomunicaciones.

en la prevención, investigación, detección y enjuiciamiento de delitos, en especial contra la delincuencia organizada.

Años después, la Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo el 25 de marzo de 2004, encargó a este mismo organismo que analizara los posibles criterios para establecer normas sobre la conservación por los prestadores de servicios de datos de tráfico de las comunicaciones (entre los que se encontraban los de geolocalización), siendo contundente el 13 de julio de 2005, a través de su declaración de condena de los atentados terroristas de Londres, cuando se reafirmó en la necesidad de adoptar, cuanto antes, medidas comunes sobre conservación de datos de telecomunicaciones, dada la importancia de los datos de tráfico y de localización para la investigación, detección y enjuiciamiento de delitos, según demostraban tanto la investigación como la experiencia práctica de varios Estados miembros al respecto, existiendo en dicha época la necesidad de asegurar a escala europea que los datos generados o tratados, en el marco de la prestación de servicios de comunicaciones, por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, se iban a conservar durante un determinado período de tiempo.

Como hemos expuesto, al haber diversa y muy distinta legislación en los Estados miembros, en relación a la conservación de datos por los prestadores de servicios para la prevención, investigación, detección y

enjuiciamiento de delitos, la Unión Europea se vio obligada a regular la materia y a armonizarla a través de la Directiva 2006/24/CE del Parlamento y del Consejo de 15 Marzo de conservación de datos generados o tratados en la prestación de servicios o redes de comunicaciones electrónicas de acceso público y modificación de la Directiva 2002/58/CE, convirtiéndose en el marco jurídico fundamental de la UE para el uso de los datos de geolocalización procedentes de dispositivos móviles inteligentes, aplicándose la modificada Directiva 2002/58/CE revisada, sobre la protección de la intimidad y las comunicaciones electrónicas, únicamente al tratamiento de datos de la estación de base por operadores de telecomunicaciones[112].

Esta Directiva 2006/24/CE, que se refiere a sólo los datos generados o tratados como consecuencia de una comunicación o de un servicio de comunicación y no a los datos que constituyen el contenido de la información comunicada[113], ha sido anulada por la reciente STJUE, Gran Sala, de 8 de abril de 2014, que trataremos posteriormente en un apartado aparte, debido a la escasa definición en la norma, de las cautelas y garantías jurídicas precisas y claras que exige la inmisión en el derecho a la protección de datos personales.

[112] Conclusión 6.1 del Dictamen 13/2011, sobre los servicios de geolocalización en dispositivos móviles inteligentes aprobado el 16 de mayo de 2011, elaborado por el Grupo de Trabajo creado en virtud del artículo 29 de la Directiva 95/46/CE, u órgano consultivo europeo independiente dedicado a la protección de datos y de la intimidad.

[113] El artículo 1 de la Directiva 2006/24/CE expone que *"se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas".*

Cronológicamente posterior, son interesantes las Conclusiones del Grupo de Trabajo sobre protección de datos del artículo 29 de la Directiva 95/46/CE o Dictamen 13/2011, sobre los servicios de geolocalización en dispositivos móviles inteligentes, aprobado el 16 de mayo de 2011[114]. Para el tratamiento de los datos[115], se requiere un consentimiento informado del usuario; así se exige que sepa claramente, como, para que, hasta cuando etc… van a ser tratados sus datos por parte de los prestadores. A la vez determina una serie de requisitos adicionales a dicho consentimiento informado para que el mismo sea plenamente válido, así, en este sentido, los requisitos más destacables, en el marco de las conexiones móviles, son los siguientes:

- La claridad de la información facilitada al usuario, para la concesión de consentimiento, de modo que un usuario medio pueda entenderla con toda facilidad.

- Finalidad del tratamiento de los datos, siendo esta única, y en caso de cambio o ampliación en los mismos, dicho consentimiento debe verse forzosamente renovado.
- Plazo de otorgamiento del consentimiento, que, aunque, en principio, sea indeterminado, es necesario renovarlo al menos anualmente.

[114] *Vid.,* UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29, Dictamen 13/2011… *op.cit.*

[115] MESEGUER GONZÁLEZ, J.D., *Derechos fundamentales afectados por la geolocalización,* Tribuna, EL DERECHO, 22 de julio de 2013.

- Especificación de los datos de localización que se conservarán; es decir, de los datos generados por el proceso de geolocalización, cuáles de ellos serán almacenados u tratados en el futuro.

El resto de servicios de valor añadido distintos de los datos de localización, en tanto se presenten accesoriamente al contenido material de la comunicación, deberán reputarse datos de tráfico. Por el contrario, si constituyen la información que el emisor pretende transmitir al receptor, su régimen habrá de ser el propio del contenido material de la comunicación, que deberá respetar, por tanto, el derecho al secreto de las comunicaciones.

Sentado lo anterior, se instituyen tres tipos de responsables del tratamiento de datos:

- Responsables del tratamiento de infraestructuras de geolocalización (en particular, los responsables del cartografiado de puntos de acceso *WiFi*).

- Proveedores de aplicaciones y servicios de geolocalización.

- Creadores del sistema operativo de dispositivos móviles inteligentes.

En cualquier caso, lo que se defiende como requisito indispensable, para que la intimidad no se vea afectada, es la necesaria existencia de un consentimiento fundamentado previo del propietario del dispositivo móvil inteligente, que nunca deberá obtenerse a través de condiciones generales; debiendo siempre ser específico para los diferentes fines para los que se procesen los datos, y pudiendo ser retirado en cualquier momento de forma fácil y sin consecuencias negativas para el uso del producto de que se trate.

No podemos olvidarnos de la regulación de los datos de geolocalización obtenidos a través de los servicios de la sociedad de la información, entendiendo por tales a las empresas que ofrecen servicios de localización y aplicaciones basadas en una combinación de datos de estaciones de base, GPS y *WiFi*, los cuales se regulan mediante la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[116], ya que quedan explícitamente excluidos de la Directiva sobre la protección de la intimidad y las comunicaciones electrónicas, en virtud de la definición estricta de "servicio de comunicaciones electrónicas" dada por la Directiva 2002/21/CE, de 7 de marzo de 2002[117].

[116] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[117] Artículo 2, letra c) de la Directiva 2002/21/CE, de 7 de marzo de 2002 del Parlamento Europeo y del Consejo, relativa a un marco regulador común de las redes y

Por último, y completando lo anterior, se elaboró por el Grupo de Trabajo del artículo 29, el Dictamen 4/2007, del 20 de junio, sobre el concepto de datos personales[118], concluyendo, entre otros, que dicho concepto no es ilimitado. Las normas comunitarias se concibieron para ser aplicadas en situaciones en las que los derechos individuales pueden correr peligro y, por tanto, necesitar protección, sin que por ello haya de llevarse a su extremo. Este análisis del Grupo de Trabajo se ha basado en los cuatro "componentes" principales que pueden distinguirse en la definición de "datos personales", esto es: "toda información", "sobre", "identificada o identificable" y "persona física", los cuales se encuentran estrechamente ligados entre sí, complementándose recíprocamente.

III.2.- Marco jurídico nacional

los servicios de comunicaciones electrónicas: *"servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos; quedan excluidos asimismo los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas"*.

[118] UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 DE LA DIRECTIVA 95/46/CE Dictamen 4/2007, del 20 de junio, sobre el concepto de datos personales.

En el ámbito nacional, la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, transpuso al ordenamiento jurídico español el marco regulador de las comunicaciones electrónicas aprobado por la Unión Europea en el año 2002, profundizando en los principios de libre competencia y mínima intervención administrativa, consagrados en la normativa anterior. Desde su aprobación y hasta su derogación, esta Ley ha sido objeto de diversas modificaciones tendentes a garantizar la aparición y viabilidad de nuevos operadores, la protección de los derechos de los usuarios y la supervisión administrativa de aquellos aspectos relacionados con el servicio público, el dominio público y la defensa de la competencia.

Actualmente, en sustitución de la anterior, la Ley 9/2014, de 9 Mayo, General de Telecomunicaciones, que persigue garantizar el cumplimiento de los objetivos de la Agenda Digital para Europa[119], que requiere, en la presente situación de evolución tecnológica e incertidumbre económica, asegurar un marco regulatorio claro y estable que fomente la inversión, proporcione seguridad jurídica y elimine las barreras que han dificultado el despliegue de redes y un mayor grado de competencia en el mercado. Esta norma refuerza los derechos de los

[119] Preámbulo II, de la Ley 9/2014, de 9 Mayo, General de Telecomunicaciones (BOE 10 de mayo de 2014)*" […] La Agenda Digital para Europa, principal instrumento para el cumplimiento de los objetivos de la Estrategia Europa 2020, persigue que para 2020 todos los europeos tengan la posibilidad de acceder a conexiones de banda ancha a una velocidad como mínimo de 30 Mbps, y que, al menos, un 50 % de los hogares europeos estén abonados a conexiones de banda ancha superiores a 100 Mbps. Estos objetivos han quedado incorporados a la agenda digital española, aprobada por el Gobierno en febrero de 2013. Para ello, según estimaciones de la Comisión Europea, se deberá invertir hasta dicha fecha una cantidad comprendida entre los 180.000 y 270.000 millones de euros. Se calcula que en España serán necesarias inversiones del sector privado por valor de 23.000 millones de euros."*

usuarios, clarificando los derechos ya introducidos, en la anterior Ley 32/2003, por el Real Decreto-Ley 13/2012, de 30 de marzo, con una mejor identificación de los mismos relacionados con la protección de datos de carácter personal y la privacidad de las personas.

Esta norma toca de manera muy tangencial e insuficiente a los datos de geolocalización, ya que, si bien, en su Anexo II –punto 9- podemos encontrar una interesante definición de la geolocalización, así presenta a los "Datos de localización" como cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público, únicamente trata directamente los mismos cuando establece que forman parte, como veremos más adelante, de la información que los operadores que explotan redes públicas de comunicaciones electrónicas, o que prestan servicios de comunicaciones electrónicas disponibles al público, han de facilitar a los agentes facultados por la orden de interceptación legal de las comunicaciones[120].

Aparte de la anterior, y como norma aplicable a esta materia, debe mencionarse la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPDCP), que deroga la LO 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de

[120] Artículo 39 de la Ley 9/2014, de 9 mayo, General de Telecomunicaciones (BOE 10 de mayo de 2014).

Carácter Personal, modificada por la Ley 2/2011, de 4 de marzo, de Economía Sostenible en su Disposición final quincuagésima sexta, y la LO 1/1982 de Protección del Honor, la Intimidad Personal y Familiar y la Propia Imagen.

No hay duda de que los datos relativos al lugar de ubicación de un objeto y al trazado de sus eventuales desplazamientos, siempre que se vincule o pueda ser vinculado a una persona física sirviendo a la identificación de esta, integra el concepto de dato de carácter personal.

Así lo entiende en diversos informes, el Gabinete Jurídico de la Agencia Española de Protección de Datos (AEPD); en ellos se precisan diferentes aspectos de los datos que permiten la localización geográfica. El citado órgano se ha pronunciado mediante sucesivos informes, entre otras materias, en relación con los datos emitidos por GPS instalados en vehículos (Informe 193/2008), la geolocalización de los accesos a portales de juego *online* (Informe 216/2008), la traslación a personas jurídicas de las normas de protección de datos en relación con los de tráfico y localización en telecomunicaciones (Informe 420/2008), la lectura de matrículas por la policía en un aparcamiento público (Informe 433/2008) o el tratamiento de datos de localización de empleados en tarea de escolta mediante los datos GPS enviados por teléfonos móviles (Informe 640/2009).

Ahora bien, para que un dato de carácter personal quede sujeto al régimen de tutela de la LOPDCP y su Reglamento, es necesario que la actuación respecto de tales datos corresponda a una operación de las incluidas en el concepto de "tratamiento"[121], entendiendo por tal, según su artículo 3.c), las *"operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*".

Los datos de localización, que sufren un tratamiento de carácter automatizado (artículo 3.1. de la Directiva 95/46/CE), integran sin duda alguna esta categoría, de ahí que consideremos que claramente se ven afectados por el derecho a la protección de datos personales o *habbeas data* consagrado en el artículo 18.4 de la Constitución Española[122].

[121] Para PÉREZ GIL, "tratamiento de datos" es una noción comprensiva de todas aquellas operaciones y procedimientos que permitan realizar al menos una de las actuaciones que mencionan los preceptos 3.c) de la LOPDCP. De ello se deriva que cualquiera de esas actuaciones (recoger, grabar, conservar, etc.) será, en sí misma, constitutiva de "tratamiento", como viene a plasmar el art. 5.1.c) RPDCP, al definir la "cesión o comunicación de datos" de la siguiente manera: "Tratamiento de datos que suponen su revelación a persona distinta del interesado".

Vid., PÉREZ GIL, J., "Los datos sobre localización geográfica…", *op.cit*.

[122] Recordado por PÉREZ GIL, el Tribunal Constitucional define este derecho en su sentencia 292/2000, FJ 5, como "*un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".* La garantía opera sobre datos de muy diversa naturaleza, siempre que "*tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado"* (sentencia del Tribunal Constitucional 292/2000, FJ 6).

Vid., PÉREZ GIL, J., "El nuevo papel de la telefonía móvil en el proceso penal…", *op.cit.*, p. 150.

Aún es más, la información relativa al lugar donde se encuentra o por donde ha pasado un concreto terminal, que siempre va a poder vincularse con su usuario, encaja también en la definición del artículo 5.1.f) de la Directiva 2006/24/CE, incorporado al artículo 3.1 f) Ley 25/2007, de 18 de octubre de conservación de datos relativas a las comunicaciones electrónicas y a las redes públicas de comunicaciones (LCDCE). Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados, siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales, siendo de expresa aplicación a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado, conforme a su artículo 1.2., siempre y cuando dicha información no forme parte del contenido de comunicación electrónica alguna.

Viene así a concluir el Tribunal Constitucional su propia doctrina, después de superar pronunciamientos que lo hacían aparecer con carácter instrumental, como garantía-presupuesto, para la protección de otros derechos.

FERNÁNDEZ LÓPEZ, J.M., *La protección de datos personales como derecho fundamental en España y en la Unión Europea: su contenido y los derechos que derivan para los ciudadanos*, en "El derecho al honor, a la intimidad y a la propia imagen. El derecho a la libertad frente al uso legítimo de la informática: planteamiento general y problemas civiles", Cuadernos Digitales de Formación, núm. 16, Consejo General del Poder Judicial, Madrid, 2008, p.3.

Impone a los operadores de comunicaciones[123] o sujetos obligados, el deber de conservar durante un plazo de doce meses[124]:

- La etiqueta de localización (identificador de celda), al inicio de la comunicación.

- Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el periodo en el que se conservan los datos de las comunicaciones.

Quedan expresamente a salvo de esta obligación, aquellos datos que revelen el contenido de la comunicación.

Según su Preámbulo, esta norma es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya

[123] Más concretamente, a los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, de conformidad con su artículo 2.

[124] Artículo 5.1 LCDCE: "*La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores".*

sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá siempre la autorización judicial previa.

En cuanto a los datos objeto de la obligación de conservación son los ya enumerados anteriormente por la Directiva 2006/24/CE, y que, en ningún caso revelarán el contenido de la comunicación, siendo los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado. Se incluyen asimismo en el ámbito de aplicación de la Ley las denominadas llamadas telefónicas infructuosas[125], así como la necesaria conservación de los elementos que sean suficientes para identificar el momento de activación de los teléfonos que funcionen bajo la modalidad de prepago[126].

Se excluyen los datos relativos a las llamadas no conectadas, que es aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

[125] Artículo 6.2 LCDCE: *"Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada".*

[126] Artículo 3.1.e)2º,vi) LCDCE: *"En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio".*

Sin perjuicio del tratamiento más pormenorizado que se dará a la regulación contenida en la Ley de Enjuiciamiento Criminal en capítulos posteriores, hemos de significar que tras su reforma operada por 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[127], se ha incluido un Capítulo dedicado a "Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos"[128], con el fin de dar cabida a la inaplazable regulación de esta materia. Se aprovecha así un esquema formal histórico que, pese a los problemas prácticos derivados de su obsolescencia, cuenta con la ventaja de haber sido objeto de frecuente atención por parte de la jurisprudencia del Tribunal Supremo[129].

[127] Criticada por autores como BUENO DE MATA. El autor espera un próximo desarrollo jurisprudencial por estimar peca de abstracta o indeterminada.

BUENO DE MATA, F., *Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica,* Diario La Ley, núm. 8627, Sección Doctrina, Ref. D-382, Editorial LA LEY, 19 octubre 2015.

[128] Las medidas de investigación tecnológica son objeto de atención en los Capítulos V a VII del Título VIII del Libro II de la Ley de Enjuiciamiento Criminal, y a todas ellas resultan de aplicación las disposiciones comunes introducidas en el Capítulo IV.

[129] Preámbulo, IV, Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (BOE núm. 239, de 6 de octubre de 2015).

III.3.- Especial referencia a la declaración de invalidez de la Directiva 2006/24/CE por la sentencia del TJUE, Gran Sala, de 8 de abril de 2014.

Como ya se ha avanzado, la Directiva 2006/24/CE fue anulada por la sentencia del Tribunal de Justicia de la Unión Europea, Gran Sala, de 8 de abril de 2014, siguiendo con ello la doctrina expuesta por la sentencia del Tribunal Constitucional alemán de 3 de marzo de 2010, lo cual merece ser comentado en relación con la norma nacional de trasposición de esta Directiva vigente en España o Ley 25/2007, de 18 de octubre de conservación de datos relativas a las comunicaciones electrónicas y a las redes públicas de comunicaciones, con análisis de los posibles efectos y consecuencias jurídicas.

Para RODRÍGUEZ LAÍNZ[130], esta Directiva ha sido sometida a un *"prolongado asedio"* que ha culminado con una más que previsible "*crónica de una muerte anunciada*", señalando como causas:

- La reticencia de algunos Estados para asumir el mandato de transposición[131].
- La tardanza de determinados Tribunales Constitucionales en la anulación de las leyes internas dictadas en su desarrollo[132].

[130] RODRÍGUEZ LAÍNZ, J.L., *Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre la conservación de datos relativos a las comunicaciones*, Diario La Ley, núm. 8308, Sección Doctrina, Ref. D-148, La Ley Unión Europea, Editorial LA LEY, 12 de Mayo de 2014.

[131] Por ejemplo, la República de Irlanda que llegó a recurrir al TJUE para impugnar la Directiva por motivos formales, siendo desestimada por STJUE de 10 de febrero de 2009.

- La visión crítica de determinados organismos a nivel interno de la propia Unión[133].
- La presión de determinados lobbies liderados por operadoras de telecomunicaciones acuciadas por el sobrecosto económico que les representaba el deber de conservación de datos.

Ha de partirse de que la Directiva es una herramienta de armonización o de acercamiento de normas nacionales, en la que se marcan los márgenes de discrecionalidad que tienen los Estados miembros para obtener unos objetivos comunes concretos así definidos[134], no existiendo con la norma nacional de transposición, una relación de interdependencia, por lo que la pérdida de validez de la norma comunitaria no ha de implicar necesariamente que la ley nacional haya de sufrir la misma suerte. Según el RODRÍGUEZ LAÍNZ[135], *"haría falta una nueva norma interna o comunitaria que así lo dispusieran, dentro de los ámbitos de sus respectivas competencias y fuerza normativa de los correspondientes instrumentos legales, para que la norma nacional perdiera su vigencia"*.

---

[132] El Tribunal Constitucional alemán, en su sentencia de 2 de marzo de 2010 (asuntos BvR 256/2008, 263/2008 y 586/2008); el Tribunal Constitucional rumano, en su Decisión 1258, de 8 de octubre de 2009; y el Tribunal Constitucional checo en su sentencia de 22 de marzo de 2010.

[133] En concreto, Informe de evaluación sobre la Directiva de Conservación de Datos, elaborado el 18 de abril de 2011, por la Comisaria de Asuntos de Interior de la Unión Europea, Dª. Cecilia Malmström. Recuperado de: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2011)0225_/com_com(2011)0225_es.pdf (última consulta: 18 de abril de 2011).

[134] Artículo 288, párrafo tercero, del Tratado de Funcionamiento de la Unión Europea.

[135] *Vid.,* RODRÍGUEZ LAÍNZ, J.L., *Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE…*, *op. cit.*

Sentado esto, y entrando al análisis concreto del contenido de la sentencia, esta determina, en un primer momento, los derechos fundamentales que se ven afectados por la Directiva. Así, tenemos el derecho al secreto de las comunicaciones, entendido en su dimensión de protección de contenidos y el derecho de protección de datos.

El secreto de las comunicaciones se relaciona con el concepto de *libertad de comunicaciones*; mostrando el Tribunal Europeo su preocupación por el sentimiento de que los ciudadanos podamos vernos compelidos en nuestra libertad de comunicación por el hecho de que seamos conscientes del rastro que dejan nuestras comunicaciones al quedar registradas y conservadas, conforme ordena la Directiva, generando con ello una sensación de vigilancia constante.

Aparte de lo anterior, la sentencia se centra en el ámbito de la privacidad, y más en concreto, de la protección de datos de carácter personal, como barrera anticipada instrumental de la primera.

La resolución plantea que la conservación preventiva de datos relativos a las comunicaciones, como por ejemplo los de geolocalización, suponen una grave restricción de los derechos[136], por lo que realiza un

[136] Sentencia del TJUE, Gran Sala, de 8 de abril de 2014, apartado 29: *"La conservación de datos para su eventual acceso por las autoridades nacionales competentes, según se establece en la Directiva 2006/24, afecta de manera directa y específica a la vida privada y, por tanto, a los derechos que garantiza el artículo 7 de la Carta. Además, el artículo 8 de la Carta también es aplicable a dicha conservación de datos, puesto que constituye un tratamiento de datos de carácter personal en el sentido*

juicio de proporcionalidad[137] y de necesidad[138] de la regulación, sopesando el interés en la represión de delitos graves y protección de la seguridad nacional, y este sacrificio (preventivo) de los ciudadanos.

La resolución concluye determinando que la normativa de la Unión debe establecer reglas claras y precisas, que regulen el alcance y la aplicación de la medida en cuestión, y establezcan unas exigencias mínimas, de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos[139].

---

de ese artículo y debe, por tanto, cumplir necesariamente los requisitos de protección de datos que se derivan de dicho artículo".

Apartado 36 de la misma sentencia: *"Asimismo, la Directiva 2006/24 constituye una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta puesto que establece un tratamiento de datos de carácter personal".*

[137] Sentencia del TJUE, Gran Sala, de 8 de abril de 2014, apartado 46: "*El principio de proporcionalidad exige que los actos de las instituciones de la Unión sean adecuados para lograr los objetivos legítimos perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos (véanse, en este sentido, las sentencias Afton Chemical, EU:C:2010:419, apartado 45; Volker und Markus Schecke y Eifert, EU:C:2010:662, apartado 74; Nelson y otros, C-581/10 y C-629/10, EU:C:2012:657, apartado 71; Sky Österreich, C-283/11, EU:C:2013:28, apartado 50, y Schaible, C-101/12, EU:C:2013:661, apartado 29".*

[138] Sentencia del TJUE, Gran Sala, de 8 de abril de 2014, apartado 51: *"En cuanto al carácter necesario de la conservación de datos que impone la Directiva 2006/24, ha de señalarse que es cierto que la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, reviste una importancia primordial para garantizar la seguridad pública y su eficacia puede depender en gran medida de la utilización de técnicas modernas de investigación. Sin embargo, este objetivo de interés general, por fundamental que sea, no puede por sí solo justificar que una medida de conservación como la establecida por la Directiva 2006/24 se considere necesaria a los efectos de dicha lucha".*

[139] Por analogía, en lo que respecta al artículo 8 del CEDH, las sentencias TEDH, Liberty y otros *vs.* Reino Unido de 1 de julio de 2008, nº 58243/00, §§ 62 y 63; Rotaru c. Rumanía, antes citada, §§ 57 a 59, y S y Marper *vs.* Reino Unido, antes citada, §§ 99.

Más concretamente, en la resolución se argumenta que la Directiva abarca, de manera generalizada, a todas las personas (incluidas también aquellas cuyas comunicaciones están sujetas al secreto profesional), medios de comunicación electrónica y datos de tráfico, sin que se realice diferenciación alguna, limitación o excepción en función del objetivo de lucha contra los delitos graves. Aparte de a esta falta de límites, la resolución hace referencia a una ausencia de criterio objetivo[140] que permita delimitar el acceso de las autoridades nacionales competentes a los datos y a su utilización posterior con fines de prevención y enjuiciamiento de delitos, así como la inexistente determinación de condiciones materiales y de procedimiento a seguir para el acceso a los datos conservados.

En lo relativo al periodo de conservación, critica que se fije un periodo genérico mínimo de seis meses, sin hacer distinción alguna entre las diversas categorías de datos, en función de su posible utilidad en relación con el objetivo perseguido o con las personas afectadas.

[140] Sentencia del TJCE, Gran Sala, de 8 de abril de 2014, apartado 62: *"En particular, la Directiva 2006/24 no establece ningún criterio objetivo que permita limitar el número de personas que disponen de la autorización de acceso y utilización posterior de los datos conservados a lo estrictamente necesario teniendo en cuenta el objetivo perseguido. En especial, el acceso a los datos conservados por las autoridades nacionales competentes no se supedita a un control previo efectuado, bien por un órgano jurisdiccional, bien por un organismo administrativo autónomo, cuya decisión tenga por objeto limitar el acceso a los datos y su utilización a lo estrictamente necesario para alcanzar el objetivo perseguido y se produzca a raíz de una solicitud motivada de dichas autoridades presentada en el marco de procedimientos de prevención, detección o enjuiciamiento de delitos. Tampoco se ha establecido una obligación concreta de los Estados miembros de que se fijen tales limitaciones".*

Por todo ello, la sentencia sostiene que la Directiva no cuenta con reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales, no conteniendo garantías suficientes, como las exigidas por el artículo 8 de la Carta, que permitan asegurar una protección eficaz de los datos conservados contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos, respecto de tales datos, sin que se haya previsto o aconsejado a los Estados miembros que establezcan tales reglas.

Así, si bien la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, tiende a copiar la literalidad del texto de la Directiva, ello no significa que adolezca de los mismos defectos, tesis que compartimos con RODRÍGUEZ LAÍNZ[141].

El legislador español, al utilizar el concepto de "...delitos graves contemplados en el Código Penal o en las leyes penales especiales", soluciona jurídicamente de manera correcta las necesidades de proporcionalidad exigidas por la sentencia.

En cuanto a la falta de determinación de criterios objetivos en la definición de las autoridades nacionales legitimadas para el acceso, ello no es predicable de nuestra legislación nacional, que somete plenamente

[141] *Vid.,* RODRÍGUEZ LAÍNZ, J.L., *Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE...*, *op. cit.*

a las garantías procesales y constitucionales cualquier recabo de datos almacenados, siempre en el contexto de un concreto proceso de investigación criminal y bajo el control de la autoridad judicial. Más aún, con la reforma sufrida en septiembre de 2015 por la Ley de Enjuiciamiento Criminal, que trataremos en profundidad más adelante, quedan claros límites, requisitos y exigencias que anteriormente solo tenían reflejo en nuestra jurisprudencia, encargada de regular *de facto* situaciones novedosas ante la pasividad del legislador reflejada en el antiguo artículo 579 de la Ley de Enjuiciamiento Criminal.

En lo relativo a los plazos de conservación, por un lado tenemos el artículo 5.1 de la Ley que establece una delegación reglamentaria que permitiría modular los plazos, solucionando así el problema y, por otro, siempre existe la posibilidad de interpretación acorde al caso concreto por parte de la autoridad competente, no recabándose más datos que aquellos referidos a los periodos temporales más acordes con la gravedad de la concreta injerencia a la que se somete a la persona investigada, como así se deduce de la nueva legislación procesal penal española.

Aparte de todo lo anterior, la legislación española garantiza los estándares de protección y seguridad de los datos conservados. No solo contamos con la Ley, sino que el nivel de seguridad ha sido elevado por el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LO 15/1999, de 13 de diciembre, de protección de datos de carácter personal, a lo que ha de unirse aparte de la

salvaguardia de la autoridad en cada caso concreto, la función de autoridad pública independiente de control atribuida expresamente a la Agencia Española de Protección de Datos[142].

Si no fuera bastante lo anterior, a través de la posibilidad de subsanación a nivel de legislación nacional, siempre podrían arbitrarse fórmulas legislativas de determinación del alcance del deber de conservación, más ajustadas a lo exigido por el Tribunal Europeo.

Tras lo expuesto, no resulta extraño el afirmar que en la actualidad las tecnologías de la información y de la comunicación han alcanzado un desarrollo incuestionable. De una parte, la expansión de las redes de telecomunicaciones supone un importante desafío para la sociedad actual, en el sentido de encontrarnos ante procesos comunicativos en el entorno informático cada vez más complejos y sofisticados, que han superado con creces a la norma, y que necesitan de una protección jurídica actualizada, ante las más que posibles amenazas emergentes en la conocida como sociedad de la información del siglo XXI.

Contamos con sistemas GPS como dispositivos autónomos y como parte integrante de nuestro dispositivo de comunicación móvil, redes *WiFi* que transmiten información de nuestra localización más allá de la que el ciudadano voluntariamente desea, archivos *Exif* en nuestras fotos que

[142] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Recuperado de: https://www.agpd.es/portalwebAGPD/index-ides-idphp.php (última consulta: 12 de enero de 2016).

integran datos de la ubicación, estaciones base de telefonía que recogen de manera constante nuestra situación espacial... múltiples variantes que merecen ser analizadas una por una, como parte de un todo, pero en compartimentos estancos, ante la gran laguna jurídica existente.

Tenemos un complejo, y veremos, escaso entramado normativo que en muy pocas ocasiones hace referencia concreta a los datos de geolocalización. Se hace preciso analizar su tipología, averiguar su naturaleza jurídica, para poder posteriormente determinar qué norma es la aplicable y si esta es bastante para lograr la seguridad jurídica que se merece el ciudadano.

CAPÍTULO II

INTERVENCIÓN/OBTENCIÓN DE LOS DATOS DE GEOLOCALIZACIÓN

La evolución de la tecnología y el desarrollo de las comunicaciones supone la aparición de un nuevo campo de investigación para las Fuerzas y Cuerpos de Seguridad del Estado. Al igual que la delincuencia hace uso de los avances tecnológicos, las unidades de investigación se valen de ellos para perfeccionar su acción y acceder a información que tiempo atrás, era imposible.

No es necesario retroceder mucho en el tiempo para darnos cuenta del desarrollo inmenso que ha experimentado el campo de la geolocalización. Para conocer la ubicación de una persona, supuesto delincuente, las unidades de investigación únicamente contaban con los tradicionales seguimientos policiales, lo cual suponía un gran despliegue de medios personales y económicos. Actualmente, la tecnología pone en su mano multitud de herramientas para la averiguación de los ilícitos y, como ya hemos visto, el ámbito de la geolocalización no se queda atrás.

Tras haber presentado los nuevos instrumentos tecnológicos que permiten acceder a la localización de una persona, así como la regulación existente al respecto, hemos de plantearnos cómo ha de lograrse dicha información en plano de respeto con los derechos constitucionales y la ley. Dicha tarea no es fácil, dado que se cuenta, como hemos visto, con múltiples posibilidades para la obtención de la geolocalización, y no existe un texto legislativo que de manera clara se ocupe de ello, encontrándonos asimismo con numerosas lagunas legales.

En este capítulo se estudiarán, desde un punto de vista jurídico, las diversas variantes con las que cuenta el investigador para la obtención de los datos de localización, en el marco de una investigación penal.

I.- DATOS DE GEOLOCALIZACIÓN DE ESTACIONES BASE TRATADOS POR OPERADORES DE TELECOMUNICACIONES

Es obvia la utilidad que para la investigación y la prueba del delito proporcionan las señales de localización derivadas del uso de la telefonía

móvil y los indicios[143] que pueden aportar, tanto si se ha establecido una comunicación como si no.

Siempre que estos indicios estén debidamente enlazados entre sí y con otros elementos relevantes, abrirán en la investigación múltiples posibilidades para desvelar hechos y descubrir a los culpables[144]. Dicha utilidad, por ejemplo, fue puesta de manifiesto durante el procedimiento judicial abierto por el atentado del 11-M[145], acreditando vínculos entre las personas implicadas.

Para poder entender, desde un punto de vista jurídico, este procedimiento de obtención y/o intervención de los datos de geolocalización derivados de las estaciones base, hemos de conocer su distinta naturaleza y para ello, hemos de partir de su ubicación, de manera genérica, dentro de la noción de "datos de las comunicaciones electrónicas".

---

[143] El término indicio entendido *"en el sentido más vulgar de sospecha, con mayor o menor fundamento, de la que se infiera racionalmente la posibilidad de que una o mas personas sean autoras de un delito determinado, con soporte en algún dato objetivo conocido"*.

HURTADO ADRIÁN, A.L., *El teléfono como medio de investigación en el proceso penal,* Actualidad Penal, núm. 1, marginal 168, Editorial LA LEY, Madrid,1994.

[144] "*De esta manera podremos por ejemplo incluir o excluir a sospechosos en las escenas del delito, verificar cortadas o contrastar versiones diferentes sobre hechos. Ciertamente con ello se pueden eludir otras formas más intrusivas de investigación y, además, hace posibles investigaciones que, de otro modo, serían poco menos que imposibles*".

Vid., PÉREZ GIL, J., "El nuevo papel de la telefonía móvil en el proceso penal…", *op.cit.*, quien recuerda a RODRÍGUEZ LAÍNZ, J.L., *Consideraciones jurídicas en torno a la licitud constitucional del SITEL*, en Diario La Ley, núm. 7544, Sección Doctrina, Año XXXI, Editorial LA LEY, 17 de febrero del 2010.

[145] Sentencia de la Audiencia Nacional, Sala de lo Penal, Sección 2ª, de 31 de Octubre de 2007.

El artículo 2.a) de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, por la que se modifica la Directiva 2002/58/CE[146], define los "datos" como *"los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario"*, realizando con ello una primera clasificación en la que parece diferenciar los datos de geolocalización, de los de tráfico, afirmación que, como veremos, no es exacta.

En cuanto a los "datos de tráfico", la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997 (derogada posteriormente), relativa al Tratamiento de Datos Personales y Protección de la Intimidad en el sector de las Telecomunicaciones[147], en su artículo 2.b) ofrece, por fin, una definición auténtica de "dato de tráfico", entendiendo por tal *"cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma"*[148].

[146] Sin perjuicio de la anulación de la Directiva 2006/24/CE por la STJUE de 8 de abril de 2014, debido a la escasa definición en la norma de las cautelas y garantías jurídicas precisas y claras que exige la inmisión en el derecho a la protección de datos personales, podemos seguir haciendo uso de las diferentes definiciones y categorías que nos ofrece.

[147] Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997 (derogada posteriormente), relativa al Tratamiento de Datos Personales y Protección de la Intimidad en el sector de las Telecomunicaciones.

[148] Esta definición se reiteró en su instrumento de transposición, concretamente en el Real Decreto 424/2005, de 15 de abril, por el que se aprobó el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (articulo 64 a).

Dicha Directiva, que fue expresamente derogada por la Directiva 2002/58/CE, del Parlamento Europeo, relativa al Tratamiento de los Datos Personales y Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas, incorporó en su Anexo una enumeración de los datos de tráfico definidos con carácter general, en el artículo 6.2 donde podía leerse: *"...a los efectos a que se hace mención en el apartado 2 del artículo 6, podrán procesarse los siguientes datos que incluyan: el número o la identificación de la estación del abonado, la dirección del abonado y el tipo de estación, el número total de unidades que deben facturarse durante el ejercicio contable, el número del abonado que recibe la llamada, el tipo, la hora de comienzo y la duración de las llamadas realizadas o el volumen de datos transmitido, la fecha de la llamada o del servicio, otros datos relativos a los pagos, tales como pago anticipado, pagos a plazos, desconexión y notificaciones de recibos pendientes"*.

Sin perjuicio de lo anterior, la realidad cambiante de las comunicaciones electrónicas ha provocado la constante ampliación de los datos incluibles en la categoría de datos de tráfico, aunque sólo sea eventualmente, debiéndose aplicar esta denominación actualmente a, no solo aquellos datos relacionados con el contenido de la comunicación, sino también a datos como los de localización o abonado[149].

[149] De ahí la definición más amplia de datos de tráfico que nos proporciona GIMENO SENDRA: *"aquellos datos que se generan o tratan en el curso de una comunicación y que difieren del contenido material, entendiendo por tal aquella información cuya transmisión voluntaria por el emisor al receptor motiva la comunicación"*.

En conclusión, y dejando a un lado lo que es la comunicación propiamente dicha o el envío voluntario de un mensaje entre el emisor y el receptor, se encuentran los datos de tráfico o también denominados "datos externos"[150]. Se dan no solo durante la existencia de la comunicación, sino también previa y posteriormente al proceso, y su trascendencia, una vez concluida la comunicación, radica precisamente en que aportan información acerca de ella, ya sea como consecuencia de que se trataron para hacer posible la comunicación o porque se transmitieron accesoriamente al contenido material, quedando aquí incluidos los datos de geolocalización de los que nos ocupamos en este apartado.

Por tanto, existen datos de geolocalización que han de ser tratados como datos de tráfico, y para ello recordamos lo ya expuesto al respecto de los mismos y, más en concreto, su definición o *"cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible al público"* (artículo 2.c) de la Directiva 2002/58/CE); la propia Directiva 2002/58/CE aclara, en su considerando 14, que tales datos pueden referirse a la latitud, la longitud

Vid., GIMENO SENDRA, V., *La intervención de las comunicaciones*, Diario La Ley, núm. 7192, Sección Doctrina, Editorial LA LEY, 9 Junio 2009, p. 6.

[150] GONZÁLEZ LÓPEZ, por su parte, distingue en el contenido de la comunicación dos vertientes, una material o el contenido de la comunicación propiamente dicho, y otra formal o datos de tráfico, también llamados datos externos.

Vid., GONZÁLEZ LÓPEZ, J.J., *Utilización en el proceso penal de datos vinculados a las comunicaciones electrónicas recopilados sin indicios de comisión delictiva*, en "Protección de datos y proceso penal", Editorial LA LEY, Madrid, junio 2010.

y la altitud del equipo terminal del usuario, a la dirección de la marcha, al nivel de precisión de la información de la localización, a la identificación de la célula de red en la que está localizado el equipo terminal en un determinado momento o a la hora en que la información de localización ha sido registrada.

Por otro lado, y dentro de la categoría de **datos de suscripción o de abonado**, definidos como aquellos que constituyen "la información personal recabada del abonado a la hora de suscribir el contrato de prestación de servicios de comunicación"[151], también podemos encontrarnos con datos de geolocalización. Tanto para disponer de una conexión telefónica, como para una conexión a Internet, es preciso celebrar un contrato con el operador de comunicaciones electrónicas o con el proveedor de acceso a Internet, debiendo proporcionar para ello determinadas informaciones personales, que no se circunscriben solo a la identificación del abonado, sino que también comprenden determinadas informaciones relativas al servicio cuya prestación se contrata, incluyendo ubicación del abonado.

Así, de acuerdo con la Memoria Explicativa del Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2011[152], los "*datos de suscripción" son "cualquier información contenida en formato*

[151] HERNÁNDEZ GUERRERO, F. J., "La intervención de las comunicaciones electrónicas", III-2001, Estudios Jurídicos, Ministerio Fiscal, 2001, p. 355, recordado por *Vid.,* GONZÁLEZ LÓPEZ, J.J., *Utilización en el proceso penal de datos…*, op.cit.

[152] Memoria Explicativa del Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2011. Recuperado de: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF (última consulta: 21 de marzo de 2015).

informático o en cualquier otra forma, que es mantenida por el proveedor de servicios, relativa a usuarios de sus servicios, distintos de los de tráfico o de contenido, por los que puede establecerse:

- *El tipo de servicio de comunicación usado, las previsiones técnicas adoptadas para ello y el período de servicio.*

- *La identidad del usuario, dirección postal o geográfica, teléfono u otro número de acceso, información sobre cuentas corrientes y pago, disponible sobre la base de un contrato de servicio o acuerdo.*

- *Cualquier otra información sobre el lugar de instalación del equipo de comunicaciones disponibles sobre la base del contrato de servicios o de un acuerdo".*

Si bien todos estos datos son previos a la comunicación, y no aparecen con motivo de las concretas operaciones técnicas necesarias para hacer factible la comunicación pretendida, sino como marco previo para que esas actuaciones se lleven a cabo, si se presentasen en el curso de la comunicación misma, tendrán la consideración de datos de tráfico[153], categoría que, como hemos dicho, cada vez aglutina un mayor número de datos.

[153] En la misma línea, *Vid.,* GONZÁLEZ LÓPEZ, J. J., *Utilización en el proceso penal de datos vinculados…*, *op. cit.*

Aparte de los anteriores datos de geolocalización, como datos de tráfico y como datos de suscripción, tenemos **"los datos de localización distintos de los de tráfico"**[154]. Se consideran actuaciones técnicas, que si bien pueden considerarse comunicación desde un punto de vista técnico, escapan al propósito de la comunicación (proceso comunicativo) y simplemente constituyen un presupuesto técnico necesario para hacerla posible.

Así, pues, no es desconocido que, al margen de las comunicaciones en curso, existe un elenco de datos, orientados a hacerlas factibles y que son distintos de los datos de suscripción, e independientes de las distintas conexiones del abonado o usuario, por ser variables en función de las diferentes conexiones del terminal. Aun cuando algunos de estos datos de localización pueden también presentarse como datos de tráfico en determinados momentos, a veces no responden a sus características, mostrando asimismo una existencia autónoma respecto de las concretas comunicaciones, pudiendo ser obtenidos de manera aislada[155].

Por último, podemos encontrar también **datos de localización como servicios de valor añadido**, los cuales cuando integran el contenido material de la comunicación, apareciendo como la información

[154] GONZÁLEZ LÓPEZ los denomina "datos operativos de puesta a disposición de los servicios de comunicaciones electrónicas".

Vid., GONZÁLEZ LÓPEZ, J. J., *Ibid.*

[155] GONZÁLEZ LÓPEZ los denomina "datos de prestación", en el bien entendido de que los datos de tráfico también obedecen a la prestación de los servicios de comunicaciones electrónicas, pero con una dimensión distinta a la de los datos a que aludimos con esa expresión

Vid., GONZÁLEZ LÓPEZ, J. J., *Ibid.*

que el emisor desea transmitir al receptor, constituyen materia de protección del artículo 18.3 Constitución Española[156] (tal es el caso, por ejemplo, de la transmisión, vía aplicación móvil *WhatsApp,* de la ubicación geográfica del usuario para su conocimiento por el receptor de la comunicación).

La **obtención de los distintos datos de geolocalización** se rige, dependiendo de la naturaleza que ostenten conforme a la clasificación anteriormente expuesta, bien por las reglas de la protección de datos de carácter personal, o bien por las reservadas a materias protegidas de manera reforzada por el artículo 18.3 Constitución Española.

En ningún caso, la obtención de estos datos de geolocalización podría vulnerar el derecho a la intimidad, ya que entendemos que ninguna afectación puede predicarse de la utilización de un método que lo único que pretende es conseguir, en un radio de acción prefijado, la activación de unos mecanismos de comunicación, traducidos en números, de donde pueda inferirse la localización de unos terminales de donde inducir la presencia de los sospechosos en un concreto lugar, teniendo presente que esa ubicación sólo puede concretarse con una

[156] RODRÍGUEZ LAÍNZ también defiende su inclusión en el contenido (material) de la comunicación cuando alcancen "sustantividad, bien por su propia naturaleza o finalidad". Esta línea es asimismo sostenida por GONZÁLEZ LÓPEZ.

Vid., RODRÍGUEZ LAÍNZ, J. L., "La intervención de las comunicaciones telefónicas", Bosch, Barcelona, 2002, p. 31 y 32.

Vid., GONZÁLEZ LÓPEZ, J. J., *Ibid.*

aproximación de varios cientos de metros, que es la zona cubierta por la BTS o estación repetidora que capta la señal[157].

En resumen, la información relativa a la localización puede convertirse en accesible por dos vías:

- La primera, en el curso de una intervención de comunicaciones a través del sistema SITEL (debiendo existir, por tanto, la preceptiva autorización judicial para la intervención). Sería aplicable a información captada con motivo de un proceso comunicativo en marcha. En este caso, los datos de ubicación formarían parte inseparable de la comunicación y, en consecuencia, han de estar amparados por el derecho al secreto de las comunicaciones recogido en el artículo 18.3 de la Constitución, constituyan o no, el contenido material de la misma.

- Y la segunda, como consecuencia del acceso a las bases de datos reguladas por el artículo 1 de la Ley 25/2007, de 18 de octubre de conservación de datos relativas a las comunicaciones electrónicas y a las redes públicas de comunicaciones (LCDCE)[158]; siendo esta última opción muy

[157] La no vulneración del derecho a la intimidad es defendida por numerosas sentencias. A modo ejemplar, sentencias del Tribunal Supremo, Sala Segunda, 706/2006, de 14 de junio, 906/2008, de 19 de diciembre o 777/2012, de 17 de octubre.

[158] La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones expresamente dispone en su artículo 42 que *"La conservación y cesión de los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente*

criticada por la jurisprudencia[159], opinión que se ha impuesto al legislador si atendemos a la nueva regulación existente en la Ley de Enjuiciamiento Criminal, tras la modificación operada por la reciente 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.

Conforme a la Ley 25/2007, de 18 de octubre, los operadores de comunicaciones tienen la obligación de conservar, durante un plazo de doce meses[160], la etiqueta de localización (identificador de celda) al inicio de la comunicación, así como los datos que permiten fijar la localización

autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones".

[159] La doctrina del Tribunal Supremo entiende que esta intromisión no puede hacerse depender de un imperativo legal, sino que siempre ha de ser el resultado de una resolución judicial motivada específicamente para la adopción de esta medida. A modo ejemplar, en esta línea, el voto particular a la sentencia del Tribunal Supremo , Sala Segunda, 316/2011, de 6 de abril, seguido por la sentencia de la misma Sala del Tribunal Supremo 286/2011, de 15 de abril. Mismo tenor fue posteriormente defendido por el voto particular a la sentencia del Tribunal Supremo, Sala Segunda, 15/2012, de 20 de enero, y por las sentencias del Tribunal Supremo, misma Sala, 67/2012, de 9 de febrero; 109/2012, de 14 de febrero; 478/2012, de 29 de mayo, y 794/2012, de 11 de octubre; hasta la más reciente sentencia del Tribunal Supremo 209/2013, de 6 de marzo.

[160] Artículo 5 de la Ley 25/2007, de 18 de octubre, de conservación de datos relativas a las comunicaciones electrónicas y a las redes públicas de comunicaciones, fija como periodo de conservación de los datos, el de 12 meses computados desde la fecha en que se haya producido la comunicación y siempre referido a delitos graves (artículo 1.1), aspecto de problemática interpretación. Por su parte, el artículo 42 dispone que *"La conservación y cesión de los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones".*

geográfica de la celda, mediante referencia a la etiqueta de localización[161]. Esta información estaría vinculada a la prestación de un servicio de comunicaciones electrónicas y que se sitúa en un momento temporalmente anterior (datos de cobertura) o posterior (datos conservados por la operadora, por el propio terminal o por sus sistemas de almacenamiento), siendo, por tanto, datos que se obtienen en un momento distinto al proceso comunicativo.

En la misma línea de esa jurisprudencia crítica y de la actual redacción de la Ley de Enjuiciamiento Criminal, autores como MARCHENA GÓMEZ[162] han resaltado la importancia de que estos datos electrónicos adquieran sustantividad jurídica propia, huyendo del actual *statu quo* en que su cesión por las operadoras de servicio a los investigadores se puede producir como consecuencia de un mandato legal, no de una resolución judicial que así lo autorice.

Más flexible se ha mostrado parte de la doctrina, así, por ejemplo, GONZÁLEZ LÓPEZ[163], defensor de que los datos de localización, cuando se tratan al margen de las comunicaciones que se realizan con el terminal al que corresponden, obedecen al propósito de poner a disposición del abonado o usuario el servicio de comunicación y, por

[161] Artículo 5.1.f) de la Directiva 2006/24/CE, incorporado al artículo 3.1 f) Ley 25/2007, de 18 de octubre de conservación de datos relativas a las comunicaciones electrónicas y a las redes públicas de comunicaciones (LCDCE), en relación con el articulo 42.

[162] MARCHENA GÓMEZ, M., *Proceso penal: nuevos problemas, viejas soluciones,* La Ley Penal, núm. 100, Sección Estudios, Editorial LA LEY, Madrid, 2013.

[163] GONZÁLEZ LÓPEZ, J. J., *Obtención de la IMSI con fines de investigación penal: Comentario a la STS 248/2008 (Sala de lo Penal, de 20 de mayo)*, Revista Jurídica de Castilla y León, núm. 23, Junta de Castilla y León, enero 2011.

tanto, están teleológicamente orientados a permitir las eventuales comunicaciones que se lleven a cabo, pero, entre tanto estas no tengan lugar, la captación de esta información no afectará, en ningún caso, al artículo 18.3 de la Constitución Española, puesto que no hay comunicación actual que salvaguardar.

Por su parte, PÉREZ GIL[164], con anterioridad a la nueva redacción del texto procesal penal, planteaba la posible afectación del derecho a la intimidad con la obtención de datos de carácter personal relativos a la localización, entendiendo que debían ponderarse los intereses en conflicto, para poder, así, fijar la línea divisoria a partir de la cual comienza la razonable expectativa de intimidad digna de tutela; critica, asimismo, las resoluciones jurisprudenciales que basan su argumento de la no vulneración de derecho alguno en el grado de precisión de la localización, toda vez que entonces, entiende el autor, que, a sensu contrario, habría de concluirse que, de lograrse una precisa localización del sujeto investigado que permitiese determinar con exactitud el lugar, edificio o vivienda en el que se hallase (lo cual es perfectamente posible con tecnología fácilmente accesible), podría vulnerarse el derecho a la intimidad[165].

[164] *Vid.,* PÉREZ GIL, J., "Los datos sobre localización geográfica…", *op. cit.*

[165] Recuerda el autor en su nota a pie 14: "La Corte Suprema de los EE.UU. se pronunció hace tiempo en relación con la utilización de dispositivos de seguimiento, distinguiendo sus efectos en espacios privados frente a espacios públicos, para lo que se sirvió como criterio delimitador de la afección a una expectativa razonable de intimidad. Así, en *United States vs. Karo* [468 U.S. 705, 714 (1984)], la Corte concluyó que el dispositivo de localización que monitorizaba los movimientos de una persona dentro de su casa afectaba a esa razonable expectativa de intimidad. En *United States vs. Knotts* [460 U.S. 276, 277 (1983)], la Policía instaló un dispositivo de localización en una lata de cloroformo que el acusado adquirió y dejó en su coche, permitiendo a la Policía así

También critica el autor la antigua practica procesal desarrollada por los instructores judiciales que autorizaban la interceptación de conversaciones telefónicas, dando por hecho que el resto de los datos electrónicos que se obtienen con esa diligencia están revestidos del mismo régimen jurídico, y se integran en el paquete cerrado del artículo 33 LGT, aconsejando aporten una motivación explícita al respecto; esto es lo actualmente exigido tras la reciente Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

En otra línea semejante, VELASCO[166] pone en duda a aquellos sectores doctrinales que equiparan la tecnovigilancia (entre los que se encuentra la geolocalización) con las tradicionales vigilancias físicas policiales (solo necesitadas de autorización judicial, cuando afectan a domicilios y lugares cerrados reservados al ejercicio de la privacidad). Entiende el autor que, por un lado, los dispositivos electrónicos que muestran la geolocalización de su usuario, a veces, suponen una injerencia en espacios privados respecto de los cuales sí sería necesaria la autorización judicial para la práctica de una diligencia de investigación (por ejemplo, el GPS de un *smartphone* emite más tiempo desde lugares

realizar un seguimiento del vehículo a través de las calles y autopistas recorridas. La Corte entendió que en este caso no sería de aplicación la 4ª enmienda, que sólo protege los espacios privados pero no los públicos".

166 VELASCO NÚÑEZ, E., *Tecnovigilancia, geolocalización y datos: aspectos procesales penales*, Diario La Ley, núm. 8338, Sección Doctrina, Año XXXV, Editorial LA LEY, 23 junio 2014.

privados, como puede ser un domicilio que desde la vía pública) y, por otro lado, cree que las conclusiones interpretativas a las que se puede llegar podrían ser erróneas ya que, siguiendo el anterior ejemplo, el teléfono móvil no es la persona y la geolocalización informa sobre la ubicación del dispositivo y no, sobre quién es la concreta persona que lo usa en casa momento. Por lo anterior, aconseja que, para evitar abusos, una ley ha de habilitar y definir, en abstracto, los supuestos en que cabe el sacrificio del derecho en aras al mayor beneficio social que supone una concreta investigación delictiva, regulando asimismo las garantías que permitan al investigado ejercer una efectiva defensa para el caso de que la investigación no sea ajustada a derecho.

La habilitación legal ha de ser previa a la injerencia investigadora y debe estar formal y materialmente regulada con cierto detalle por una norma que persiga un fin legítimo, con rango de ley, que determine, entre otros, los supuestos habilitantes, la duración y el procedimiento de obtención, custodia, análisis, uso penal, cesión a otras investigaciones, e incluso, de destrucción de la información así obtenida.

Todo lo anterior, por fin, ha culminado en la esperada previsión expresa, por parte de la Ley de Enjuiciamiento Criminal, de la posible obtención por los investigadores, mediante previa solicitud de autorización judicial, de "la localización geográfica del origen o destino de

la comunicación"[167], de lo cual se deduce la necesidad de resolución judicial en forma de Auto para la concesión de dicha información por las operadoras. Se responde así al requerimiento efectuado por jurisprudencia y un gran sector doctrinal[168] que tildaba de insuficiente la regulación.

I.1.- Datos de geolocalización como datos de tráfico

La clave interpretativa ofrecida por la jurisprudencia del TEDH ha resultado decisiva para afianzar el espacio de exclusión del secreto de las comunicaciones, extendiendo su ámbito a datos externos o datos de tráfico que no tienen por qué trascender a terceros ajenos al proceso de comunicación, pero requieren el mismo nivel de protección que el contenido de aquélla.

[167] Artículo 588 ter d 1c) de la Ley de Enjuiciamiento Criminal.

[168] "Este bloque normativo no cuenta con el mínimo grado de precisión necesario para regular la utilización de diligencias que, como sucede en un requerimiento de cesión de datos, llevarán implícita una restricción del derecho a la protección de datos personales por nimia que pudiera ser. Tales previsiones establecen con carácter general habilitaciones o deberes (colaboración o denuncia, respectivamente), pero van referidas a todas y cada una de las distintas diligencias de investigación penal en las que cupiera pensar. No se olvide, además, la necesidad de propiciar de seguridad jurídica a los receptores del requerimiento, pues independientemente de su disposición a colaborar voluntariamente con las autoridades encargadas de la investigación penal, precisan un claro soporte legal que les libere de eventuales responsabilidades contractuales o extracontractuales. Por ello, nuestro criterio en relación con las cesiones inconsentidas de datos es que las normas procesales deberían aportar certidumbre sobre las pautas necesarias para establecer concretos parámetros, requisitos específicos o mecanismos de control (judicial o no) a los que se deba ajustar un requerimiento de cesión de datos personales en el marco de la investigación de hechos delictivos.[…] Lo lógico sería que los requerimientos judiciales de cesión de datos de carácter personal se encontrasen contemplados por la norma procesal penal, entre las diligencias de investigación de la LECrim."

Vid., PÉREZ GIL, J., *Los datos sobre localización geográfica…*, *op. cit.*

La solución ofrecida en 1984 en el caso Malone[169], tanto por su singularidad, como por el estado de los avances técnicos en la fecha en que aquella fue pronunciada, sólo pudo referirse a algunos datos muy concretos relacionados con la técnica del recuento -*open register o comptage*-[170]. Su afirmación de que los números de teléfono marcados, la hora y la duración de la llamada forman parte de los datos externos al proceso de comunicación, pero requieren el mismo nivel de protección que el contenido de aquélla, siendo decisiva, sólo resuelve una pequeña parte del problema.

Hoy en día la telefonía móvil, como ya hemos podido ver, genera toda una serie de datos de tráfico que van mucho más allá de aquellos respecto de los que el TEDH tuvo ocasión de pronunciarse, hace ahora más de 29 años, como pueden ser los datos de geolocalización anexos al proceso comunicativo.

A la luz de la tan mentada sentencia del caso Malone, nacieron otras resoluciones como la STEDH de 1 de julio de 2008, caso Calmanovici *vs.* Rumania, asunto 42250/02, que dio definitivamente

[169] STEDH de 2 de agosto de 1984, caso Malone *vs.* Reino Unido.

[170] Según se precisa en el apartado 56 de la mencionada resolución, el recuento consiste en *"...el uso de un instrumento -un contador combinado con un aparato impresor- que registra los números marcados en un determinado aparato telefónico y la hora y la duración de cada llamada"*. Añade el Tribunal que *"...el recuento es distinto por su propia naturaleza de la interceptación de las comunicaciones, la cual y en principio, no es deseable ni lícita en una sociedad democrática. El Tribunal no acepta, sin embargo, que la utilización de los datos así obtenidos no pueda plantear problemas en relación con el artículo 8. En los registros así efectuados, se contienen informaciones -en especial, los números marcados- que son parte de las comunicaciones telefónicas. En opinión del Tribunal, ponerlos en conocimiento de la Policía, sin el consentimiento del abonado, se opone también al derecho confirmado por el artículo 8"* (apartado 84).

carta de naturaleza, aunque de forma prácticamente implícita, a la extensión de su doctrina al concepto más amplio del dato de tráfico, al incluir dentro del ámbito de la protección del artículo 8.1 del CEDH la conservación de estos datos obtenidos en una interceptación y su eventual utilización en un procedimiento penal contra la persona concernida[171].

De la simple lectura de esta sentencia y de la larga lista de resoluciones de las que trae causa, se puede deducir la confusión entre el ámbito de protección de los datos de carácter personal y del derecho al secreto de las comunicaciones, toda vez que ambos derechos son descritos en cualquier injerencia sobre el proceso comunicativo como si de una sola realidad jurídica se tratara. Asimismo, existen numerosas resoluciones del Tribunal Europeo en las que efectivamente, no solo el contenido, sino incluso el dato relacionado con una comunicación consumada y conservada, no ya en archivos informáticos de operadores

[171] Ello ha sido criticado por autores tales como RODRÍGUEZ LAÍNZ, quien no se muestra conforme con que el TEDH hagan participar de la misma realidad jurídica y ámbito de protección, los derechos a la vida privada y al secreto de la correspondencia, debido a la inexistencia de una referencia explícita a la protección de los datos de carácter personal, como nexo de unión de lo que son verdaderos ámbitos de protección formal y material del más amplio derecho a la privacidad: *"Se echa de menos, sin duda, en esta jurisprudencia una visión conjunta del mundo de las comunicaciones con los datos de carácter personal tan intrínsecamente relacionados con éstas, como sí se puede apreciar en la legislación comunitaria.[…] Fuera de toda controversia doctrinal o jurisprudencial sobre la materia, resulta evidente que la actual normativa comunitaria, de la que se extrae claramente la diferencia entre lo que es comunicación y dato asociado a ésta, de lo que es dato de carácter personal relativo a una comunicación ya consumada, no solo regula sino que impone tal diferenciación de tratamiento; y es de esperar que en próximas resoluciones del TEDH, llegue a acogerse tal distinción, lejos de las especiales circunstancias en las que hubo de examinarse el supuesto de hecho del caso Wieser y Bicos Beiligungen GMBH v. Austria, o el contexto de poder de control y disciplina en materia de relaciones laborales en que se contextualizó la STEDH de 3 de abril de 2007 (caso Copland vs. Reino Unido; asunto 62617/00).".*

Vid., RODRÍGUEZ LAÍNZ, J. L., *Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas*, en "Estudios sobre el secreto de las comunicaciones. Perspectiva doctrinal y jurisprudencial", 1ª edición, Editorial LA LEY, Madrid, diciembre 2011.

de comunicaciones, sino del propio destinatario, mantienen la protección dispensada por el Convenio al derecho al secreto de la correspondencia privada[172].

Todo cuanto antecede advierte que el concepto de datos externos manejado por el TEDH, en la tantas veces invocada sentencia del Caso Malone, ha sido absolutamente desbordado por una noción más amplia, definida por la locución "datos de tráfico", en cuyo ámbito se incluyen elementos de una naturaleza y funcionalidad muy heterogénea. En este sentido, tan dato de tráfico sería, por tanto, el número de abonado con el que se conecta un terminal telefónico, como el número de IMSI asociado a éste, que permite que la llamada llegue a su destino; y cómo no, la dirección de correo electrónico desde la que se emite un mensaje, como la concreta dirección IP desde la que se accede al servidor en el que está alojada la cuenta de correo electrónico, incluyendo los datos de geolocalización.

Entendemos que estos datos no afectan al contenido de la comunicación ni al núcleo duro de la intimidad, de modo que, en todo caso, su ámbito de protección sería el correspondiente al derecho a la protección de datos, sin que se pueda ver afectado el derecho fundamental al secreto de las comunicaciones. Ello no obsta para que hayan de obtenerse dichos datos con las cautelas legales precisas, no

[172] STEDH de 16 de octubre de 2007, caso Wieser y Bicos Beiligungen GMBH *vs.* Austria; asunto 74336/01.

pudiendo entenderse como bastante el seguimiento de un simple trámite meramente administrativo para su obtención, como plantea GIMENO[173].

En esta línea de superación del caso Malone también nos encontramos con resoluciones del Tribunal Supremo[174], el cual considera que la mecánica importación del régimen jurídico de aquellos datos a estos otros puede conducir a un verdadero desenfoque del problema, incluyendo en el ámbito de la protección constitucional del derecho al secreto de las comunicaciones, datos que merecen un tratamiento jurídico diferenciado, en la medida en que formarían parte, en su caso, del derecho a la protección de datos o, con la terminología de algún sector doctrinal, del derecho a la autodeterminación informativa (artículo 18.4 de la Constitución Española). Para afirmar esto, el Alto Tribunal se basa en criterios de "funcionalidad" y "accesoriedad", conceptos claves para determinar el alcance de la tutela constitucional de la que gozan.

Esta opinión jurisprudencial ha sido duramente criticada por GONZÁLEZ LÓPEZ[175] que califica este planteamiento como

[173] GIMENO SENDRA recuerda que la mayoría de las legislaciones europeas prevén la posibilidad de intervenciones "administrativas" de las comunicaciones, y plantea como opción para la descongestión de los Juzgados de Instrucción, y de cara a aumentar la eficacia de las investigaciones electrónicas, otorgar la facultad de dictar las autorizaciones para la intervención de los datos de tráfico al Ministerio Fiscal, entendiendo que dicha intervención en nada afecta al derecho al secreto de las comunicaciones, comparándolo, a modo de ejemplo, con la lectura por el cartero del destinatario y remitente de una carta impresa.

Vid., GIMENO SENDRA, V., *Las intervenciones electrónicas y la policía judicial*, Diario La Ley, núm. 7298, Sección Tribuna, Año XXX, Ref. D-378, Editorial LA LEY, 4 diciembre 2009.

[174] Sentencia del Tribunal Supremo, Sala Segunda, 249/2008, de 20 de mayo.

[175] *Vid.*, GONZÁLEZ LÓPEZ, J. J., *Obtención de la IMSI con fines de investigación penal…, op. cit.*

"cuestionable", dado que es un planteamiento claramente restrictivo, que, además de excluir datos de tanta trascendencia como los de localización (cuando son datos de tráfico), no es congruente con la insuficiencia que el tribunal atribuye al concepto "datos externos" empleado por el TEDH ni con el alcance del derecho al secreto de las comunicaciones que se proyecta "*a cualquier forma de interceptación en el proceso de comunicación mientras el proceso está teniendo lugar, siempre que sea apta para desvelar, ya sea la existencia misma de la comunicación, el contenido de lo comunicado o los elementos externos del proceso de comunicaron"*. Entiende el autor que con este planteamiento quedan excluidos, del ámbito de protección del derecho previsto en el artículo 18.3 de la Constitución Española, ciertos tipos de datos en función de la clase de información que aportan, aplicando un criterio hermenéutico que, por su dimensión material, es propio del derecho a la intimidad, y que resulta contrario al carácter formal que el Tribunal Constitucional (en sentencias como la 114/1984, de 29 de septiembre y siguientes) ha atribuido a este derecho, llegando, así, a una del todo inadecuada inseguridad jurídica ante la constante ampliación de informaciones accesorias al contenido material de la comunicación.

Para el autor[176], los datos de tráfico hacen referencia a una realidad definida fundamentalmente por un factor temporal y por otro volitivo. El hecho de la comunicación es el origen de estas dos categorías:

[176] *Vid.,* GONZÁLEZ LÓPEZ, J. J., *Utilización en el proceso penal de datos vinculados…*, *op. cit.*

el contenido y los datos de tráfico. Ambas, en realidad, integran el contenido de la comunicación, en el que es posible diferenciar una vertiente material (a la que normalmente se califica de contenido) y otra formal (los datos externos, o, más correctamente los datos de tráfico). Esta vinculación a la comunicación en curso no significa que sólo existan durante el transcurso de ésta, ya que de hecho, muchos de los datos que se califican de tráfico existen con anterioridad, y lo mismo puede decirse de la información que constituirá el contenido material. Asimismo, también es frecuente que perduren más allá de la comunicación. Sin embargo, el hecho de que aparezcan vinculados a una comunicación es lo que les confiere una naturaleza especial, ya que, a partir de esa vinculación, y con posterioridad a ella, harán referencia o estarán conectados, a un fenómeno concreto: la transmisión de información del emisor al receptor (la comunicación), lo cual explica su interés para la investigación penal. Por lo que respecta a los datos de tráfico, su trascendencia, una vez concluida la comunicación, radica precisamente en que aportan información acerca de ella, ya sea como consecuencia de que se trataron para hacer posible la comunicación, o porque se transmitieron accesoriamente al contenido material.

No podemos mostrarnos de acuerdo con las anteriores afirmaciones. Si bien los datos de geolocalización como datos de tráfico se encuentran vinculados con la comunicación, ello no les confiere una naturaleza especial que merezca la protección reforzada del artículo 18.3 de la Constitución Española. Que exista vinculación entre ellos no puede

confundirnos, y llevarnos a igualarlos. Los datos de geolocalización, en este caso, van en paralelo con la comunicación propiamente dicha dentro del proceso comunicativo, pero no forman parte del mensaje que el emisor voluntariamente transmite al destinatario. No es comunicación, por tanto, aunque caminen de la mano en estos casos. Es por ello que no tienen la misma naturaleza, ni la misma protección, pero esto no significa que su obtención y/o intervención no deba ser objeto de amparo.

Se deduce, por ejemplo, de la Directiva 2006/24/CE[177] sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, que se refiere a sólo los datos generados o tratados como consecuencia de una comunicación o de un servicio de comunicación (amparados por la protección de los datos de carácter personal) y no, a los datos que constituyen el contenido de la información comunicada, cuyo acceso ilegítimo sí podría afectar a los derechos fundamentales de los ciudadanos, al respeto de la vida privada y de las comunicaciones.

Parece que el legislador consciente de las distintas interpretaciones existentes, motivadas por una regulación insuficiente sobre la materia, por fin se ha decidido a plasmar en una norma los requisitos legales

[177] Sin perjuicio de la anulación de la Directiva 2006/24/CE por la STJUE de 8 de abril de 2014, debido a la escasa definición en la norma de las cautelas y garantías jurídicas precisas y claras que exige la inmisión en el derecho a la protección de datos personales, podemos seguir haciendo uso de las diferentes definiciones y categorías que nos ofrece.

necesarios para la interceptación de los datos de tráfico. Así hemos podido observarlo, en primer lugar, en el Anteproyecto de la Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación (a fecha 5 de diciembre de 2014)[178]. Posteriormente este Anteproyecto fue sustituido por el Proyecto de Ley Orgánica, aprobado el Pleno del Congreso el 2 de junio de 2015, que culminó en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, que actualmente dota de contenido a la materia en la nueva redacción de la Ley de Enjuiciamiento Criminal, la cual acoge el criterio fijado por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, e impone la exigencia de autorización judicial para su cesión a los agentes facultados.

Con la nueva redacción de la Ley de Enjuiciamiento Criminal ya en vigor, y dada por el artículo único catorce de la LO 13/2015, queda claro que su incorporación al proceso solo se autoriza cuando se trate de la investigación de un delito que, por razones vinculadas al principio de proporcionalidad, sea de los que justifican el sacrificio de la inviolabilidad de las comunicaciones. Se da un tratamiento jurídico individualizado al

[178] Anteproyecto de la Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación (a fecha 5 de diciembre de 2014).

acceso por agentes de policía al IMSI, IMEI, dirección IP y otros elementos de identificación de una determinada tarjeta o terminal, en consonancia con la jurisprudencia del Tribunal Supremo ya consolidada sobre esta materia. También se regula el supuesto de la cesión de datos desvinculados de los procesos de comunicación concernientes a la titularidad o identificación de un dispositivo electrónico, a los que podrá acceder el Ministerio Fiscal o la Policía Judicial, en el ejercicio de sus funciones, sin necesidad de autorización judicial.

Esta nueva regulación refuerza la línea de distinción clara entre la comunicación propiamente dicha y los datos de tráfico, al realizar menciones individualizadas respecto de los mismos, de lo que se deduce que, si bien están "asociados al proceso de comunicación", no se identifican con él.

Obtención de los datos de geolocalización. Deber de conservación de los datos por los prestadores de servicios.

El momento de aparición de los indicios[179] delictivos (ya sean referidos a la investigación o a la prevención penal) en relación con el de

[179] *"Por indicio hemos de entender todo rastro, vestigio, huella, circunstancia y, en general, todo hecho conocido, o mejor dicho, debidamente comprobado, susceptible de llevarnos, por vía de inferencia, al conocimiento de otro hecho desconocido."* Sentencia del Tribunal Supremo, Sala Segunda, 548/2009, de 1 junio, FJ 1.

Por "indicio racional de criminalidad" se entiende a las sospechas fundadas o verosímiles sobre la participación de una persona en los hechos objeto de investigación penal. Sentencia del Tribunal Supremo, Sala Segunda, 123/2001, de 4 de junio, FJ5.

Conforme a Auto de Tribunal Supremo, Sala Segunda, de 18 de junio de 1992, los indicios son *"indicaciones o señas, o sea, datos externos que, apreciados judicialmente, conforme a normas de recta razón, permiten descubrir o atisbar, como dice la doctrina*

existencia de los datos es el determinante para la exposición de este punto, de modo que:

- Si los datos requeridos de geolocalización existieran ya con anterioridad a la concurrencia de indicios criminales, su obtención se realizaría mediante su necesaria cesión de datos por los prestadores de servicios, obligadas a la conservación de datos, conforme veremos; de este modo, se trata de acreditar la vinculación de unos indicios con una información ya existente.

- Si la obtención o conservación de los datos de geolocalización se produce tras la aparición de indicios delictivos, estaríamos ante la diligencia de intervención de los datos de tráfico, orientada a recabar información futura que se vincula a un hecho investigado o que se trata de prevenir.

Las diferencias legales y técnicas que existían entre disposiciones nacionales sobre conservación de datos con fines de prevención, investigación, detección y enjuiciamiento de delitos crearon obstáculos en el mercado interior de las comunicaciones electrónicas. Como ya se ha avanzado, los prestadores de servicios debían cumplir requisitos diferentes en cuanto a los tipos de datos de tráfico y de localización que

científica, sin la seguridad de la plenitud probatoria pero con la firmeza que proporciona una sospecha fundada, es decir, razonable, lógica, conforme a las reglas de la experiencia, la responsabilidad criminal de la persona en relación con el hecho posible objeto de investigación".

debían conservarse, así como en cuanto a las condiciones y los períodos de conservación.

Recordamos que hubo que esperar a la Directiva 2006/24/CE del Parlamento y del Consejo de 15 Marzo de conservación de datos generados o tratados en la prestación de servicios o redes de comunicaciones electrónicas de acceso público y modificación de la Directiva 2002/58/CE[180], para encontrar el marco jurídico fundamental de la UE para el uso de los datos de geolocalización procedentes de dispositivos móviles inteligentes, aplicándose la modificada Directiva 2002/58/CE revisada, sobre la protección de la intimidad y las comunicaciones electrónicas, únicamente al tratamiento de datos de la estación de base por operadores de telecomunicaciones[181]; dispone en su artículo 1 que *"se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas".*

[180] Sin perjuicio de la anulación de la Directiva 2006/24/CE por la reciente STJUE de 8 de abril de 2014, debido a la escasa definición en la norma de las cautelas y garantías jurídicas precisas y claras que exige la inmisión en el derecho a la protección de datos personales, podemos seguir haciendo uso de las diferentes definiciones y categorías que nos ofrece.

[181] Conclusión 6.1 del Dictamen 13/2011, sobre los servicios de geolocalización en dispositivos móviles inteligentes.

Conforme a la anterior, son **objeto de conservación** los datos[182] de tráfico y de localización sobre personas físicas y jurídicas y los datos relacionados necesarios para identificar al abonado o al usuario registrado, en concreto, entre otros, los datos necesarios para identificar la localización del equipo de comunicación móvil, entendiendo como tales: 1) la etiqueta de localización -identificador de celda- al comienzo de la comunicación y 2) los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones (no inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación).

En el ámbito nacional, dentro de la facultad de los Estados miembros reconocida por la anterior para adoptar medidas legislativas relativas al derecho de acceso y de utilización de los datos, por parte de las autoridades nacionales, tal como determinen los mismos, se elaboró la **Ley 25/2007 de 18 de octubre de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones**.

Según su Preámbulo, esta norma es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las

[182] "Datos" referido a los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario -artículo 2 de la Directiva 2006/24 CE del Parlamento y del Consejo de 15 Marzo de conservación de datos generados o tratados en la prestación de servicios o redes de comunicaciones electrónicas de acceso público y modificación de la Directiva 2002/58/CE-.

comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores de su contenido. Una segunda garantía consiste en que la cesión de los datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

Esta Ley se aprobó con la finalidad de fijar la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por ellos, con el fin de posibilitar que dispongan de ellos los agentes facultados por un período de doce meses computados desde la fecha en que se haya producido la comunicación (artículo 5). A este respecto se entienden por *agentes facultados* los miembros de los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de Inteligencia para llevar a cabo una investigación de seguridad amparada en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. También están facultados para esta misión, los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como Policía Judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. Se trata, pues, de que todos estos agentes

puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet, pero siempre buscando el imprescindible equilibrio entre esta obligación de las operadoras y el respeto de los derechos individuales que puedan verse afectados, como por ejemplo los relativos a la privacidad y la intimidad de las comunicaciones.

Los **sujetos obligados** son los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, que deberán conservar los datos, como regla general, en los términos de la LGT.

En cuanto a los **datos objeto de la obligación de conservación**, son los fijados por la Directiva 2006/24/CE, y que, en ningún caso revelarán el contenido de la comunicación, siendo los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio y el equipo de comunicación, utilizado por los usuarios. Se incluyen, asimismo, en el ámbito de aplicación de la Ley, las denominadas llamadas telefónicas infructuosas[183], así como la necesaria conservación de los elementos que sean suficientes para identificar el

[183] Artículo 6.2: *"Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada".*

momento de activación de los teléfonos que funcionen bajo la modalidad de prepago[184].

Se excluyen los datos relativos a las llamadas no conectadas, que es aquella comunicación, en el transcurso de la cual, se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la misma y a los efectos de la investigación de que se trate, así como, a la naturaleza y complejidad técnica de la operación. Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro del plazo de 7 días naturales contados a partir de las 8:00 horas del día natural siguiente a aquel en que el sujeto obligado reciba la orden[185].

Conforme al objeto de la Ley, artículo 1, existe el deber de cesión de dichos datos a los agentes facultados siempre que sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

---

[184] Artículo 3.1.e)2º,vi): *"En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio".*

[185] Este artículo 7.3 ha sido modificado conforme al apartado dos de la disposición final cuarta de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. Anteriormente el plazo para la cesión era de 72 horas.

Para identificar dichos delitos graves, hemos de acudir al criterio penológico expuesto en el artículo 13 del Código Penal, el cual dispone que son delitos graves las infracciones que la ley castiga con pena grave, debiendo entender que aquí están incluidas todas las penas enumeradas en el artículo 33.2 del Código Penal[186] y, muy especialmente la de prisión superior a cinco años.

Lo anterior se ha convertido en la práctica en un auténtico límite para los Juzgados a la hora de autorizar la cesión de datos a los agentes facultados, debido a que muchos de los delitos que se pretenden investigar y que se realizan a través de Internet, no alcanzan en sus penas los cinco años de prisión[187].

Completando la anterior regulación, la Ley de Enjuiciamiento Criminal, tras Ley Orgánica 13/2015, de 5 de octubre, de modificación de

[186] Artículo 33.2 del Código Penal: *"Son penas graves:*

a) La prisión superior a cinco años.

b) La inhabilitación absoluta.

c) Las inhabilitaciones especiales por tiempo superior a cinco años.

d) La suspensión de empleo o cargo público por tiempo superior a cinco años.

e) La privación del derecho a conducir vehículos a motor y ciclomotores por tiempo superior a ocho años.

f) La privación del derecho a la tenencia y porte de armas por tiempo superior a ocho años.

g) La privación del derecho a residir en determinados lugares o acudir a ellos, por tiempo superior a cinco años.

h) La prohibición de aproximarse a la víctima o a aquellos de sus familiares u otras personas que determine el juez o tribunal, por tiempo superior a cinco años.

i) La prohibición de comunicarse con la víctima o con aquellos de sus familiares u otras personas que determine el juez o tribunal, por tiempo superior a cinco años.

j) La privación de la patria potestad".

[187] Así ocurre con las amenazas –artículo 169 del Código Penal- donde únicamente las condicionales en su grado máximo alcanzarían ese límite de cinco años, con las injurias y calumnias –artículos 206 y 209 del Código Penal-, con la venta o exhibición de material pornográfico entre menores –artículo 186 del Código Penal- o con el tipo básico de estafa –artículo 249 del Código Penal-.

la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica[188] prevé la conservación de los datos, sin perjuicio de que estos solo podrán ser cedidos para su incorporación al proceso con autorización judicial, incluyéndose no solo aquellos que consten en los archivos automatizados de los prestadores de servicios, sino también la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

Entendida como medida de protección, es acertada la exigencia de autorización judicial para la cesión de estos datos. En concreto, los datos de geolocalización registrados y sistematizados (de forma continua o indefinida) por las estaciones base permitiría crear el perfil de una persona concreta, afectándose con ello la vida privada del investigado[189]. Aún es más, la geolocalización, como información técnica de las operadoras, obtenida para la realización de las comunicaciones, no puede incluirse entre los datos cuyo público conocimiento entra dentro de la *expectativa razonable*, ya que el afectado no puede razonablemente pensar que con los millones diarios de comunicaciones que se producen, sus datos de geolocalización se van a conocer y singularizar, de modo que no podría ser aplicable en ningún caso la teoría de la expectativa razonable de privacidad[190].

[188] Artículo 588ter j de la Ley de Enjuiciamiento Criminal.

[189] STEDH *Rotaru vs. Rumania,* de 4 de mayo de 2000, y *Amman vs. Suiza,* de 15 de febrero de 2000.

[190] El origen de la doctrina jurisprudencial de la expectativa razonable de privacidad podemos encontrarlo en el caso Katz *vs.* US (Caso Katz v. US, 389 U.S. 347(1967),

http://supreme.justia.com/cases/federal/us/), donde el ciudadano estadounidense Sr. Katz fue enjuiciado basándose en, entre otras, la prueba consistente en la colocación por agentes, de un dispositivo electrónico (micrófono) en las cercanías de una cabina que iba a ser usada por el sospechoso, de modo que consiguen grabar una conversación que posteriormente resulta vital para fundamentar su condena.

El Tribunal Supremo de USA vio la necesidad de introducir un nuevo juicio de valor de la constitucionalidad de la injerencia, denominado *reasonable-expectation-of-privacy test* o Katz test, por el cual un ciudadano no puede ser sometido a una injerencia sobre su privacidad con la que no pudiera contar en términos razonables, dándose así por primera vez carta de naturaleza a la privacidad como derecho inherente a la persona frente a cualquier clase de intrusión.

La primera vez que el TEDH utilizó de forma expresa, la doctrina de la expectativa razonable de confidencialidad fue con su sentencia STEDH, Gran Sala, de 25 de junio de 1997 (caso Halford v. Reino Unido; 20605/1992), entendiendo el tribunal que se había vulnerado la expectativa razonable de privacidad con la que contaba la interesada al haberse intervenido dos líneas de teléfono en el puesto de trabajo de una alto cargo, habiendo sido una de ellas asignada para su uso privado. Posteriormente, fue usada dicha doctrina por el Alto Tribunal (en el ámbito de la protección del derecho a la propia imagen, las SSTEDH, Secc. 3.ª, de 25 de septiembre de 2001 (caso P.G. y J.H. v. Reino Unido; asunto 44787/1998), y Secc. 4.ª, de 28 de enero de 2003 (caso Peck v. Reino Unido; asunto 44647/1998), se volvió a hacer uso la doctrina sobre la expectativa razonable de privacidad.), hasta llegar a la mas característica de sus resoluciones en esta materia STEDH, Secc. 4.ª, de 3 de abril de 2007 (caso Copland v. Reino Unido; asunto 62617/2000), cuyo paralelismo con la sentencia del Tribunal Constitucional 241/2012, de 17 de diciembre, (que posteriormente trataremos) es innegable. En este caso el tribunal, tras afirmar que las llamadas telefónicas que proceden de locales profesionales pueden incluirse en los conceptos de "vida privada" y "correspondencia" a efectos del articulo 8.1, así como los correos electrónicos enviados desde el lugar de trabajo y la información derivada del seguimiento del uso personal de Internet, considera que la recurrente podía razonablemente esperar que se reconociera el carácter privado de sus llamadas efectuadas desde la sede laboral, por lo que hubo injerencia en su derecho fundamental. El tribunal recuerda que la utilización de información relativa a la fecha y duración de las conversaciones telefónicas y en particular los números marcados, puede plantear un problema en relación con el articulo 8 dado que dicha información es "parte de las comunicaciones telefónicas" (Sentencia Malone *vs.* Reino Unido, de 2 de agosto de 1984 (TEDH 1984, 1) serie A, núm. 82, ap.84), teniendo misma consecuencia el almacenamiento de datos personales relativos a la vida privada de una persona. En consecuencia, se considera por el tribunal que la recogida y almacenamiento de información personal relativa a las llamadas telefónicas, correo electrónico y navegación por Internet de la afectada, sin su conocimiento, constituye una injerencia en su derecho al respeto de su vida privada y su correspondencia.

Posteriormente en la STEDH, Secc. 5ª, de 2 de septiembre de 2010 (caso Uzun *vs.* Alemania; asunto 35625/2005), valoró la interferencia en el derecho a la vida privada de los particulares por la sistemática recopilación y almacenamiento de datos por los servicios de seguridad respecto de particulares, incluso sin el uso o cobertura de métodos de vigilancia. Así, entre otras medidas de vigilancia discreta, analizaba la utilización de un dispositivo GPS en vehículo usado por amigo de un sospechoso de pertenecer a un grupo terrorista, valorando precisamente el objeto del litigio desde el punto de vista de la expectativa razonable de privacidad, llegando a la conclusión de que, aparte de que la legislación alemana regulaba el supuesto de manera especialmente detallada, permitiendo de este modo la posibilidad de previsión por parte de los ciudadanos, el método empleado era de todo punto proporcionado para la finalidad perseguida; toda vez que suponía una menor inmisión sobre la intimidad del investigado que un seguimiento visual permanente, o la instalación de dispositivos de grabación de sonido, o interceptación de comunicaciones.

Por último, en la más reciente STEDH, Secc. 1ª, de 14 de marzo de 2013 (caso BernhLarsen Holdingy otros *vs.* Noruega; asunto 24117/2008), el principio de la expectativa razonable de privacidad, aunque implícitamente, fue una de las claves de la

En esta misma línea, VELASCO[191] defiende que la doctrina de terceros, sentada inicialmente por la sentencia *Smith vs Maryland* 442 US 735 (1969)[192], según la cual, lo revelado a terceros (de lo que son nuestras propias comunicaciones) no está amparado constitucionalmente

---

decisión del tribunal. El interesado, una vez que se le informó que iba a ser sometido a una inspección fiscal, que, según la legislación noruega abarcaría a los archivos contenidos en los sistemas informáticos de la empresa, tuvo un año para separar los archivos propios frente a los de las empresas que compartían el servidor, transcurriendo el plazo sin hacer nada, de modo que ha de atenerse a las consecuencias jurídicas de su obrar, asumiendo por sus propios actos la inclusión del correo incluso confidencial, tanto propio como ajeno, en el objeto de la inspección fiscal.

En el ámbito nacional, la sentencia del Tribunal Constitucional 241/2012, de 17 de diciembre, se plantea la posible vulneración de los derechos a la intimidad personal (artículo 18.1 de la Constitución Española) y al secreto de las comunicaciones (artículo 18.3 de la Constitución Española) por parte de una empresa al acceder ésta a los ficheros informáticos en que quedaban registradas las conversaciones de carácter íntimo mantenidas entre dos trabajadoras, a través de un programa de mensajería ("Trillian") instalado por ellas mismas en un ordenador de uso común y sin clave de acceso.

En relación a la posible afectación del derecho a la intimidad personal, niega el tribunal cualquier vulneración dado que fueron ambas trabajadoras quienes realizaron actos dispositivos que determinaron la eliminación de la privacidad de sus conversaciones, al incluirlas en el disco del ordenador en el cual podían ser leídas por cualquier otro usuario, pudiendo trascender su contenido a terceras personas, como aquí ocurrió al tener conocimiento la dirección de la empresa. Por tanto, fueron ellas las que, con sus propios actos, provocaron con su voluntaria actuación que no se vea afectado su derecho a la intimidad al posibilitar el conocimiento de las conversaciones por otro usuario del ordenador, trabajador de la empresa, que casualmente y sin ninguna intencionalidad tuvo acceso a todo su contenido, lo que finalmente provocó la intervención empresarial.

En relación al derecho al secreto de las comunicaciones del artículo 18.3 CE, y más concretamente en relación con la utilización de ordenadores u otros medios informáticos de titularidad empresarial por parte de los trabajadores, se afirma por el tribunal que la utilización de estas herramientas está generalizada en el mundo laboral, correspondiendo a cada empresario, en el ejercicio de sus facultades de autoorganización, dirección y control fijar las condiciones de uso de los medios informáticos asignados a cada trabajador.

La sentencia, aunque no lo refleja expresamente, es evidente que emplea el criterio de la expectativa razonable de privacidad para llegar a la conclusión de que no cabía apreciar afectación del derecho a la intimidad; desde el momento en que *"…fue la propia demandante y otra trabajadora quienes realizaron actos dispositivos que determinaron la eliminación de la privacidad de sus conversaciones, al incluirlas en el disco del ordenador en el cual podían ser leídas por cualquier otro usuario, pudiendo trascender su contenido a terceras personas, como aquí ocurrió al tener conocimiento la dirección de la empresa".* Se habla por ello de una voluntaria actuación, que habría dejado libre el acceso a sus compañeros a aquello que se conservaba en la unidad C del PC.

AGUSTINA, J. R., *Sobre la utilización oculta de GPS en investigaciones criminales y detección de fraudes laborales. Análisis jurisprudencial comparado en relación con el derecho a la intimidad*, La Ley Penal, núm. 102, Sección Estudios, Editorial LA LEY, mayo-junio 2013.

[191] *Vid.*, VELASCO NÚÑEZ, E., *Tecnovigilancia, geolocalización y datos…*, *op.cit.*

[192] Caso Smith *vs.* Maryland 442 US 735 (1969). Recuperado de: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=442&invol=735 (última consulta: 17 de febrero de 2014).

(porque, efectivamente, se trata de derechos renunciables), en la era digital debe reconsiderarse (voto reservado de la Juez Sotomayor en la sentencia *US v Jones*[193]), pues muchos de los que se ceden por el interlocutor lo son a los únicos efectos de que se establezca la comunicación y, de ello, no se puede inferir razonablemente ni voluntariedad, ni consentimiento tácito alguno.

Por todo lo anterior, el autor, en claro acierto y adelantándose a la legislación actual vigente, aconsejaba la petición de la información y el control de la misma a un Juez, debiendo ser, en todo caso, la medida necesaria (sin alternativas menos gravosas) y proporcional, y reservada solo a la investigación de infracciones graves, con solicitud y concesión por escrito, con identificación de los solicitantes y, siempre quedando constancia de la misma en la propia causa penal. Su autorización entendía había de estar motivada, desechando fines prospectivos, y debe ser notificada, cuando proceda, al afectado, quien podrá acceder a la vía del recurso y, en cualquier caso, podrá instar la destrucción de la información en un tiempo razonable.

Un único "*pero*" planteamos a lo anteriormente expuesto, y ello mostrándonos conformes con lo expuesto por VALLÉS[194]; así nos cuestionamos la eficacia de la obligatoriedad de la autorización judicial

[193] Caso United States *vs.* Jones 10-1259 (2011). SUPREME COURT OF THE UNITED STATES. Recuperado de: https://www.supremecourt.gov (última consulta: 17 de febrero de 2014).

[194] VALLÉS CAUSADA, L. M., "La policía judicial en la obtención de inteligencia…", *op.cit.*, p.430-431.

en casos de urgencia vital. Como defiende el autor, en consonancia con RODRÍGUEZ LAÍNZ, sería completamente necesario que la Policía Judicial pudiese contar con la posibilidad de efectuar un requerimiento de cesión urgente de los datos, en situaciones excepcionales de urgencia vital o riesgo catastrófico, siempre con respeto al principio de proporcionalidad, informando de ello, en el plazo más breve posible, a la autoridad judicial[195].

I.2.- Datos de geolocalización como datos incluidos en el proceso de comunicación

Los datos de localización, cuando integran el contenido material de la comunicación, apareciendo como la información que el emisor desea transmitir al receptor, constituyen por sí mismos el mensaje protegido por el artículo 18.3 de la Constitución Española[196] (tal es el caso, por ejemplo, como ya hemos expuesto, de cuando se transmite vía aplicación

[195] *"Es evidente que el procedimiento de urgencia no está orientado a eludir la acción de este último sino, dadas las circunstancias, a actuar de acuerdo con la proporcionalidad de unas medidas previstas para atender dinámicamente y con toda urgencia, situaciones de claro carácter excepcional y grave, dándole inmediata cuenta de lo actuado junto con la documentación que le permita instaurar, a la mayor brevedad, su eficaz control jurisdiccional sobre lo ya iniciado, así como la tutela judicial efectiva de los actores del suceso con todas sus consecuencias, incluida la declaración de la eventual improcedencia de lo actuado"*

Vid., VALLÉS CAUSADA, L. M., ibíd., p.432.

[196] RODRÍGUEZ LAÍNZ, J. L., "La intervención de las comunicaciones…", *op. cit.*, p. 31 y 32, que defiende su inclusión en el contenido (material) cuando alcancen "sustantividad, bien por su propia naturaleza o finalidad". Esta línea es también sostenida por GONZÁLEZ LÓPEZ.

Vid., GONZÁLEZ LÓPEZ, J. J., "Utilización en el proceso penal de datos vinculados…", *op. cit.*

Telegram, dentro de una conversación, la ubicación geográfica del usuario plasmada en un detallado plano con precisión GPS para su conocimiento por el receptor de la comunicación).

Asimismo también puede darse el caso de que la obtención o la obligación de conservación de los datos se produzca tras la aparición de indicios delictivos y se acuerde judicialmente la diligencia de intervención de las comunicaciones, orientada a recabar información futura que se vincula a un hecho investigado o que se trata de prevenir. En este caso, el sistema de intervención de las comunicaciones SITEL, además de utilizarse para la captación de las comunicaciones por las Fuerzas y Cuerpos de Seguridad del Estado, previa autorización judicial al respecto, mantiene el control en el tiempo y aporta la geolocalización de los terminales electrónicos interceptados, incluso durante los períodos en que no se esté entablando conversación alguna.

En los casos en que exista mandamiento judicial que permita sacrificar el derecho al secreto de las comunicaciones, junto a la válida injerencia del contenido de la telecomunicación (en cualquiera de sus formas, telefónica, *SMS*, *WhatsApp*, correo electrónico, *Skype*, videoconferencia, etc.), el razonamiento judicial habilitador ha de servir para autorizar el conocimiento de todos los datos asociados a la misma que señale el mandamiento (ya sean de tráfico, de localización o incluso contractuales), tal y como reconocen expresamente el párrafo 8 y el 5 del artículo 39 Ley 9/2014, de 9 de mayo, de Telecomunicaciones, que

expresamente señala que entre los datos que los sujetos obligados "deben facilitar" a los agentes facultados, cuando hay una orden de interceptación, está, letra i), la "información de la localización" y su párrafo 7 que obliga a informar "de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada", y en caso de servicios móviles, "la posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, la localización y tipo de la estación base afectada"[197].

En esta misma línea parece continuar la vigente Ley de Enjuiciamiento Criminal[198], como expondremos más detalladamente en el próximo capítulo, En efecto, admite que la autorización judicial de las comunicaciones abarque no solo el acceso al contenido de las comunicaciones propiamente dichas, sino también a los datos electrónicos de tráfico o asociados al proceso de comunicación.

[197] VELASCO NÚÑEZ, E., *Tecnovigilancia, geolocalización y datos…*, *op. cit.*

[198] Artículo 588 ter b de la Ley de Enjuiciamiento Criminal: "*2. La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario.*

También podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad.

A los efectos previstos en este artículo, se entenderá por datos electrónicos de tráfico o asociados 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".

I.2.A.- Deber de colaboración en la interceptación de las comunicaciones. Ley 9/2014, de 9 Mayo, General de Telecomunicaciones

Sustituyendo a la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se publica la Ley 9/2014, de 9 Mayo, General de Telecomunicaciones, que impone el deber especifico de colaborar de los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, delimitando el alcance de las obligaciones, tanto generales como de servicio público, que se imponen a los mismos.

Estos operadores deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias. Están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de Ley Orgánica[199].

[199] Artículo 39.1 y 39.2 de la Ley 9/2014, de 9 Mayo, General de Telecomunicaciones. Nótese que no ha sido modificada la redacción pese a la entrada en vigor de 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, y se mantiene la referencia al artículo 579.

Puede ser objeto de interceptación cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información, pudiendo realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, éste podrá ser determinado dinámicamente, cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

Este acceso servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica intervenida y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición, los datos indicados en la orden de interceptación legal, entre los que puede figurar la *información de localización*[200]. Asimismo, además de esta información relativa a la interceptación, deberán entregar, siempre y cuando conste en la orden de interceptación, la "información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada"[201].

Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de identidad de extranjero o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

[200] Artículo 39.5 i) de la Ley 9/2014, de 9 Mayo, General de Telecomunicaciones.
[201] Artículo 39.7 de la Ley 9/2014, de 9 Mayo, General de Telecomunicaciones.

Los sujetos obligados deberán tener en todo momento preparado una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que se establezcan por el Ministerio de Industria, Energía y Turismo.

En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.

A este deber de colaboración se hace referencia en la Ley de Enjuiciamiento Criminal, tras Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, en su artículo 588 ter e[202].

[202] Artículo 588 ter e de la Ley de Enjuiciamiento Criminal: *"Deber de colaboración.*
1. Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona

De la lectura del mismo, concluimos que como critica que si bien es acertado que asocie de manera expresa el delito de desobediencia al incumplimiento de este deber, se echa en falta que la norma prevea las frecuentes situaciones en las que el obligado a colaborar está fuera del territorio nacional y resulta, llamémoslo dudoso por la falta de concreción, la previsión que realiza señalando como sujeto obligado a "*toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual*", lo cual adolece de la necesaria seguridad jurídica puesto que se manifiesta como un auténtico *cajón de sastre*.

I.2.B.-Sistemas de interceptación

Las redes (cable ADSL u onda *WiFi*) por las que circula la información, contienen rastros cuya trazabilidad (seguimiento, búsqueda de conexiones, origen, etc.) permite, a veces, obtener elementos y evidencias que pueden ayudar en la investigación penal, especialmente,

que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones.

2. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades.

3. Los sujetos obligados que incumplieren los anteriores deberes podrán incurrir en delito de desobediencia.".

en los puntos en que abocan las transmisiones de todos los dispositivos conectados a una misma línea (*routers*), las que posibilitan conexiones que pueden ayudar a sentar localizaciones (conexiones *WiFi*, BTS), las *urls* que llevan al servidor o lo interpretan, los *logs* de los servidores, las *html*, que indican la estructura de una Web, los protocolos *peer to peer*, las *cookies*, ficheros que permiten acceder a determinadas Web y almacenan y recuperan información sobre hábitos de navegación de su usuario o equipo y que podrían servir incluso para reconocerle, los archivos temporales, etc.

El cuestionamiento del actual sistema legal de intervención de comunicaciones electrónicas no ha tenido su origen en un radical cambio de rumbo jurisprudencial, en la evolución de la doctrina científica, ni en la habilidad de abogados especializados en crimen organizado en su recurrente búsqueda de nuevos resquicios en los que fundamentar sus escritos de recurso, sino que ha sido la contienda política, que enfrenta a los dos principales partidos a nivel estatal la que abriera una brecha capaz de crear en la sociedad y, más en concreto, en determinados grupos de opinión (medios de comunicación, asociaciones de internautas, …) una sensación de absoluta impunidad y clima de generalizada trasgresión de los más elementales derechos fundamentales relacionados con la esfera de la privacidad de los ciudadanos en el campo de las comunicaciones electrónicas[203], pasando de ser totalmente desconocido a

[203] RODRÍGUEZ LAÍNZ, J. L., *Consideraciones jurídicas…*, *op. cit.*, p. 2.

una especie de Leviatán institucional, capaz de tener controlada a toda la sociedad lejos de la existencia de un control judicial realmente efectivo.

El interés que representa la intervención de las comunicaciones no es exclusivo de nuestro país, sino que es común a todos los de nuestro entorno cultural y tecnológico, habiendo salido a la luz, recientemente, sistemas que han gozado del más absoluto secretismo.

Así, diseñado por la Agencia de Seguridad Nacional de Estados Unidos, ECHELON es el sistema de vigilancia más importante del mundo. El embrión de la red de espionaje norteamericano data del inicio de la guerra fría, cuando un primer pacto de recogida y de intercambio de informaciones denominado "Ukusa", se estableció entre el Reino Unido y Estados Unidos. A estos dos países se unieron Canadá, Australia y Nueva Zelanda. A partir de los años 70, las estaciones de escucha implantadas en estos países empezaron a captar las señales retransmitidas hacia la Tierra por los satélites tipo INTELSAT e Inmarsat, así como un centenar de satélites de observación que "escuchan" las ondas: radio, teléfonos móviles, etc. El sistema ECHELON fue concebido como forma de interconectar todos los sistemas de escucha para permitirles funcionar como componentes de un todo integrado. Las estaciones de recepción por satélite captan el conjunto de los haces de satélites INTELSAT, la más importante de las cuales está localizada en Menwith Hill, Inglaterra, situada bajo el control directo de la NSA (Agencia de Seguridad Nacional).

Como respuesta al ECHELON, surgió en el ámbito de la Unión Europea el ENFOPOL[204], como una serie de requisitos técnicos para que las operadoras de telefonía adecuasen sus sistemas, ante eventuales demandas de "pinchazos" por parte de la policía. Su establecimiento fue ratificado por todos los países miembros en 1995, si bien no se dio a conocer hasta 1998, cuando los periodistas de *Telepolis.de* (publicación electrónica alemana) Christiane Schulzki-Haddouti y Erich Moechel iniciaron una serie de artículos sobre el tema detallando los planes para la creación de una masiva red de escuchas en la Unión Europea, publicando en su integridad diversos documentos relacionados con la creación de ENFOPOL.

Aparte de las anteriores, y como muestra del uso generalizado, se atribuyen también redes parecidas en Francia (Frenchelon), Rusia (Sorm) o Suiza (Satos-3), entre otras.

Mencionado brevemente el panorama internacional de los sistemas de interceptación, pasamos al nacional tratando las tres herramientas con las que contamos: SITEL, GOLF y SILC.

a) SITEL

[204] Su nombre deriva del inglés "*enforcement pólice"* medidas policiales o aplicación policial.

a.1.- Características técnicas del sistema SITEL

Puede ser definido como un Sistema de Interceptación Legal de Telecomunicaciones para las Fuerzas y Cuerpos de Seguridad del Estado, de ámbito nacional y de grabación centralizada, destinado a la interceptación legal de la telefonía móvil GSM y de la red fija de telefonía; en la actualidad, está dando servicio de interceptación de comunicaciones móviles, tanto de voz como de datos IP[205], así como de comunicaciones fijas de diferentes compañías.

El programa SITEL[206] es una implementación cuya titularidad ostenta el Ministerio del Interior desde el 2001; está formado por dos sistemas idénticos, pero de utilización independiente (uno para el Cuerpo Nacional de Policía y otro para la Guardia Civil), compuestos, cada uno, por un centro de recepción[207] enlazado con las salas de monitorización[208]

[205] BARRADO CASADO, M. A., *La captación de datos e intervención de las comunicaciones. Una visión técnico-policial*, en "Interceptación de las comunicaciones y nuevas tecnologías", Cuadernos Digitales de Formación, núm. 43, Consejo General del Poder Judicial, Madrid, 2010, p.11.

[206] El programa SITEL utiliza los Sistemas *Evident* para intervenir las llamadas en aquellos números de abonado para los que se ha obtenido la oportuna orden judicial. Tras su recepción en los sistemas *Evident*, las transmisiones se procesan y los datos resultantes se guardan en dos servidores y se crea una *sesión* en la base de datos que recoge información asociada a la transmisión. Todos los ficheros de la transmisión así como el contenido de la llamada se guardan en el servidor de almacenamiento. *Evident Operator*es la aplicación utilizada por los operadores para visualizar las sesiones de la base de datos y el contenido de las escuchas, y está diseñada para efectuar de manera rápida y eficaz el análisis de las sesiones recogidas por las diversas unidades que la componen. En la actualidad no se tienen previsto nuevas mejoras de este sistema ya que la empresa ETI dispone de una nueva versión denominada X-STREAM.

[207] Este Centro está enlazado con las redes de los operadores y es donde se procesan y almacenan las comunicaciones interceptadas (voz, mensajes cortos SMS, datos GPRS/UMTS…) y la información asociada a la interceptación (números intervinientes en la comunicación, fecha y hora del inicio de la llamada, duración de la misma, así como el IMEI, IMSI y localización de la celda que gestiona la llamada del teléfono intervenido).

distribuidas por todo el país. Su desarrollo responde a la necesidad de articular un mecanismo moderno, automatizado, simplificador y garantista de la figura o concepto jurídico de la intervención de las comunicaciones.

Para poder entender mejor el debate que se ha suscitado en torno a este sistema, se hace necesario fijar cuáles son las **características técnicas del sistema SITEL** y, para ello, entre otros, acudimos a la sentencia del Tribunal Supremo, Sala Segunda, 250/2009, de 13 de marzo.

El sistema se articula en tres principios de actuación:

1. Centralización: El servidor y administrador del sistema se encuentra en la sede central de la Dirección General de la Guardia Civil y en la Policía Nacional, distribuyendo la información aportada por las operadoras de comunicaciones a los distintos usuarios implicados.

2. Seguridad: El sistema establece numerosos filtros de seguridad y responsabilidad, apoyados en el principio anterior. Existen 2 ámbitos de seguridad:

[208] Desde estas salas, los usuarios operativos autorizados efectúan la escucha en tiempo real o acceden a la información almacenada en el centro de recepción de las interceptaciones de los objetivos que tienen asignados.

Nivel central: existe un ordenador del sistema para cada sede reseñada, dotado del máximo nivel de seguridad, con unos operarios de mantenimiento específicos, donde se dirige la información a los puntos de acceso periféricos, de forma estanca. La misión de este ámbito central es almacenar la información y distribuirla.

Nivel periférico: el sistema cuenta con ordenadores únicos para este empleo en los grupos periféricos de enlace en las Unidades encargadas de la investigación y responsables de la intervención de la comunicación; están dotados de un sistema de conexión con la sede central propio y seguro. Se establece una codificación de acceso por el usuario autorizado y una clave personal, garantizando la conexión al contenido de la información autorizado para ese usuario concreto, siendo necesario que sea componente de la Unidad de investigación encargada y responsable de la intervención.

3. Automatización: El sistema responde, por una parte, a la necesidad de adaptación al uso de nuevos dispositivos de almacenamiento y, por otra, a la necesidad de modernizar el funcionamiento de las intervenciones de las comunicaciones, dotándolo de un mayor nivel de garantía y seguridad, a la vez que se reducen los costes y el espacio de almacenamiento.

El sistema, en la actualidad, aporta la siguiente información relativa a la intervención telefónica:

1. Fecha, hora y duración de las llamadas.
2. Identificador de IMEI y número de móvil afectado por la intervención.
3. Distribución de llamadas por día.
4. Tipo de información contenida (SMS, carpeta audio, etc.)[209]

En referencia al contenido de la intervención de la comunicación, y ámbito de información aportada por el sistema, se verifica los siguientes puntos:

1. Repetidor activado y mapa de situación[210].

[209] Existen cinco tipos de sesiones: 1) *Sesiones de voz*. Incluyen audio y por regla general se trata de una conversación entre dos personas, pudiéndose acceder asimismo a un audio en tiempo real (o escucha de conversación en tiempo real) 2) *Sesiones de Internet.* Estas sesiones contienen páginas web o correos electrónicos, 3) *Sesiones de Fax.* Estas sesiones contienen una o varias páginas de fax, 4) *Sesiones de Módem.* Estas sesiones pueden contener varios tipos de datos, incluyendo fax e Internet. Si el módem accede a un boletín de noticias, el contenido de la llamada será un script completo para reproducir la interacción del usuario, incluyendo los ficheros bajados, 5) *Sesiones CRI*. Sesiones creadas cuando no existe contenido de llamada, como en las intervenciones de mensajes cortos *sms* ,que se envían como parte de la configuración de la llamada, 6) *Sesiones de Vídeo*. Sesiones que contienen ficheros de vídeo, como llamadas de vídeo de teléfonos de 3G.

Con cada una de estas sesiones se podrá: 1) editar una sinopsis o resumen, 2) redactar una transcripción, 3) imprimir su contenido.

En relación con las transcripciones, éstas son redactadas en documentos que utilizan el procesador Microsoft Word, y son denominadas de manera automática por el *Evident Operator*, que las guarda en la ubicación correcta para que queden así vinculadas con la sesión correspondiente.

Asimismo el sistema posee un detector de códigos DTMF, con el que es posible detectar cualquier tecla que haya sido pulsada durante la sesión y se podrá emplear para la detección de códigos de acceso o contraseñas y los menús seleccionados por el llamante.

2. Número de teléfono que efectúa y emite la llamada o contenido de la información.
3. Contenido de las carpetas de audio (llamadas) y de los mensajes de texto (SMS).

Solicitada la intervención de la comunicación y autorizada esta por la autoridad judicial competente con el empleo del programa SITEL, la operadora afectada inicia el envío de información al servidor central donde se almacena a disposición de la unidad encargada y solicitante de la investigación de los hechos, responsable de la intervención de la comunicación.

Los enlaces punto a punto establecidos, permiten únicamente la entrada de información procedente de la operadora, la cual, automáticamente, es almacenada por el sistema central en el formato recibido, con características de "solo lectura", sin intervención de los agentes facultados y queda guardada con carácter permanente en el sistema central de almacenamiento, a disposición de la autoridad judicial.

Para garantizar el contenido de la información, dichos ficheros son firmados digitalmente; se usa el formato de firma electrónica denominado *PKCS&7 Dctache*, y se utiliza, igualmente, un certificado *Camerfirma* (como entidad certificadora autorizada) emitido para el Cuerpo Nacional

[210] La aplicación *Evident Operator* permite la creación de un informe donde consten los identificadores de células y sus posiciones por cada número objetivo (incluyendo los números llamados y la fecha y hora de las llamadas).

de Policía o Guardia Civil, y que se asocia a la máquina SITEL para que pueda firmar de forma desasistida los ficheros relativos al contenido e información asociada de la interceptación. Una vez que en el sistema central se realiza el proceso de firma, se genera un nuevo fichero que contendrá la firma electrónica[211] y que verificará tanto el contenido de la comunicación, como los datos asociados a la misma[212].

El acceso, por parte del personal de la unidad solicitante, se realiza mediante código identificador de usuario y clave personal. Realizada la supervisión del contenido, se actúa igual que en el modo tradicional, confeccionando las diligencias de informe correspondientes para la autoridad judicial[213]. La evidencia legal del contenido de la intervención es aportada por el servidor central, responsable del volcado de todos los datos a formato DVD para entrega a la autoridad judicial pertinente, constituyéndose como la única versión original. De este modo, según la sentencia del Tribunal Supremo 250/2009, el espacio de almacenamiento se reduce considerablemente, facilitando su entrega por la unidad de

[211] BERNING PRIETO explica que *"SITEL cuenta con un sistema de firma electrónica reconocida, que genera para cada archivo, una firma que garantiza la autenticidad e invariabilidad del mismo, de tal suerte que el archivo de firma puede confirmar que el archivo que contiene la comunicación intervenida no ha sido vulnerado".*

BERNING PRIETO, A. D., *La intervención de las comunicaciones electrónicas,* Revista Aranzadi Doctrinal núm. 3/2012, parte Estudio, Editorial Aranzadi, Pamplona, 2012.

[212] Sentencia del Tribunal Supremo, Sala Segunda, 849/2013, de 12 de noviembre.

[213] La aplicación *Evident Operator* contiene una función especial para exportar a una carpeta o soporte de almacenado como un CD aquella información considerada como prueba judicial. Toda la información contenida en una línea u objetivo puede ser objeto de exportación, así como es posible la selección previa de las sesiones a exportar. Con la exportación se crean una serie de ficheros html con información y vínculos a los ficheros de datos (éstos en formatos habituales del sistema Windows). El índice de toda la información exportada se podrá ver al abrir el fichero Index.

investigación a la autoridad judicial competente, verificándose que en sede central no queda vestigio de la información.

Más concretamente, y en relación con la localización en SITEL, este sistema muestra no una localización exacta del dispositivo, sino información sobre conexión a las antenas BTS de las compañías móviles: hora a la que se produce la conexión a una antena, la identificación de la misma y sus coordenadas UTM, y el ángulo de conexión a la antena[214].

a.2.- Legalidad del SITEL

Si algo ha caracterizado el devenir de la crónica jurisprudencial, en relación con el SITEL, ha sido su sometimiento a un auténtico asedio por parte de abogados, quienes una y otra vez, han probado suerte cuestionando todos y cada uno de los planteamientos en que se fundamenta la estructura esencial del sistema[215]. Cada vez que una

[214] Expone VALLÉS más detalladamente: *"En una primera fase de gabinete, se trata de delimitar el sector que cubre la celda problema. Si el teléfono móvil estuviera en movimiento durante la conversación, gracias a la orientación de los sucesivos sectores de las BTS que activara, podría estimarse una determinada ruta. En esta fase se estudia también si el terminal móvil ha recibido cobertura de otras BTS, complementándose los anteriores trabajos con un estudio del solapamiento de las coberturas del conjunto de las BTS intervinientes.*

En una segunda fase, sobre el terreno, el tiempo real y sobre un terminal parado, el investigador pertrechado con un interrogador IMSI/IMEI y un amplificador, recorre el sector acotado en la fase de gabinete. Así, se captan todos los IMSI e IMEI de la operadora que se está buscando hasta que, finalmente, se capte el IMSI e IMEI del concreto terminal intervenido

A continuación debe realizarse un análisis de la intensidad de la señal y su vector de orientación para aumentar la precisión sobre la situación del emisor. […]".

Vid., VALLÉS CAUSADA, L. M., "La policía judicial en la obtención de inteligencia…", *op. cit.*, p.412-413.

[215] Las innovaciones tecnógicas han supuesto un incesante cuestionamiento del sistema, según GÓMEZ-ANGULO.

nueva sentencia del Tribunal Supremo hacía permeable más información sobre su funcionamiento, surgían nuevas líneas de cuestionamiento.

a.2.1.- Sentencia del Tribunal Supremo 1215/2009, de 30 de diciembre

La explicación técnica del sistema es una constante en resoluciones que tomaron el referente de la sentencia del Tribunal Supremo 250/2009, Sala Segunda, de 13 de marzo, ya mencionada anteriormente. Meses después, y volviendo al caso concreto del SITEL, la doctrina mayoritaria planteada en la sentencia del Tribunal Supremo 1215/2009, de 30 de diciembre, estimó la legalidad del sistema SITEL con argumentos tales como que dicho sistema de grabación es de alta seguridad, y de muy difícil, por no decir imposible, manipulación, sin que la persona que la realice sea detectada por su clave y personalmente identificada, con mayor seguridad que en un sistema tradicional de cintas analógicas. Se afirma, asimismo, en la sentencia que la manipulación del contenido de los discos de DVD[216], que es también más

GÓMEZ-ANGULO RODRÍGUEZ, M. J., *Limitaciones de derechos fundamentales en la investigación en el proceso penal y las nuevas tecnologías. Entradas y registros en lugar cerrado, intervenciones de comunicaciones y especial referencia a la toma de muestras de ADN.*, Ponencia impartida en el curso "Actuaciones del Juzgado de Guardia. Supuestos procesales y soluciones", Alicante, 22 de marzo de 2012, Plan Territorial de la Comunidad Valenciana, Consejo General del Poder Judicial, 2012, p.12.

[216] "*El contenido de los DVD sobre los que se han volcado las grabaciones impresas en el disco duro, gozan de presunción de autenticidad, salvo prueba en contrario. Se trata de documentos cuya fuerza probatoria es indiscutible y así se admite por la jurisprudencia de esta Sala al permitir en su día, la aportación del contenido de las grabaciones en formato cassette. La fuerza probatoria está avalada incluso legalmente acudiendo cumplimentariamente a la Ley de Enjuiciamiento Civil. Este cuerpo legal establece, en el caso de los documentos públicos (artículo 318), la admisión de los soportes digitalizados, dejando a salvo, como es lógico la posible impugnación de su autenticidad (artículo 267 Ley Enjuiciamiento Civil). En estos casos la ley contempla la posibilidad de llevar a los*

difícil que con el sistema anterior, si bien no es descartable, ha de ser demostrada con datos objetivables e irrefutables y planteada como objeción, a partir del momento en que se alza el secreto de las grabaciones y las partes tienen expedita la vía para solicitar su audición.

a.2.2.- Voto particular de la sentencia del Tribunal Supremo 1215/2009

Frente a lo anterior, se erige el voto particular formulado por el magistrado D. Manuel Marchena, al que se adhiere D. José Manuel Maza; el contenido esencial de este voto particular se refiere a las **garantías de autenticidad exigibles a los DVD** puestos a disposición del Juez instructor por los agentes de policía, en los que se contienen las conversaciones telefónicas de los imputados, o se da respuesta, en el plano estrictamente jurídico, a un problema procesal, esto es, al valor probatorio atribuible, desde la perspectiva de su autenticidad, a la prueba electrónica[217].

autos el original, copia o certificación del documento con los requisitos necesarios para que surta sus efectos probatorios." Fj1, C), 16.

[217] Voto particular formulado por D. Manuel Marchena, al que se adhiere D. José Manuel Maza, pronunciado en sentencia del Tribunal Supremo, Sala Segunda, 1215/2009, de 30 de diciembre, apartado I: "*Cuando se nos pide un pronunciamiento acerca de la cuestionada autenticidad de unos DVD -en este caso, ofrecidos por la Policía- nuestra respuesta no puede consistir en un acto de fe inspirado por las excelencias del software del que se valen los agentes. Tampoco podemos incorporar al objeto del debate el grado de confianza institucional que a la Sala le merezca el trabajo de las Fuerzas y Cuerpos de Seguridad del Estado. Algunos pasajes de la sentencia ("... la autenticidad del contenido de los discos está fuera de discusión. Si en alguna ocasión las partes personadas estiman que los discos depositarios de la grabación no responden a la realidad, deberán explicar suficientemente en qué basan su sospecha en cuanto que están acusando de un hecho delictivo a los funcionarios que se encargan del control del sistema SITEL") desenfocan el núcleo del problema, convirtiendo lo que debería ser un debate genuinamente jurídico en un juicio sobre la credibilidad que nos inspira la labor de las Fuerzas y Cuerpos de Seguridad del Estado.*

Entienden que la atribución de eficacia probatoria a los DVD (expresamente impugnados en su autenticidad por la defensa de uno de los recurrentes), supone un retroceso respecto del estado actual de las garantías constitucionales (artículos 18.3 y 24.2 de la Constitución Española) y que esa relajación del nivel de exigencia que el Tribunal Supremo y la jurisprudencia constitucional habían venido imponiendo, se produce en una materia (la prueba electrónica) caracterizada precisamente por su volatilidad y por las infinitas posibilidades de manipulación y tratamiento.

Defienden que, si bien su fuerza probatoria no tiene por qué ser cuestionada a priori en aquellos casos en los que se impugne su exactitud e integridad en momento procesal oportuno (se incluye el escrito de conclusiones provisionales), surge en la acusación el deber de desplegar un esfuerzo probatorio que acredite, sin perjuicio de las dificultades inherentes a una prueba pericial sobre esta materia, que esa objeción de la defensa no resulta justificada y, como fundamento demostrativo, aluden a precedentes dictados en relación a soportes convencionales de escuchas telefónicas, así por todas, sentencias del Tribunal Supremo, Sala Segunda, 1075/2004, 24 de septiembre y 1566/2005, 30 de diciembre; añaden, además, que no

Y no es esto lo que está en juego. El enunciado del problema es mucho más sencillo. Lo que se requiere de nosotros no es que avalemos la suficiencia técnica del procedimiento mediante el que se graban las conversaciones intervenidas. Tampoco que examinemos el funcionamiento del sistema con la perspectiva de su validez en el ámbito de la protección de datos personales. Nuestro razonamiento, por el contrario, no puede tener otro objetivo que dar respuesta, en el plano estrictamente jurídico, a un problema procesal, esto es, al valor probatorio atribuible, desde la perspectiva de su autenticidad, a la prueba electrónica".

existen razones jurídicas que justifiquen que el resultado de los actos de investigación encomendados a las Fuerzas y Cuerpos de Seguridad del Estado se sustraigan a las reglas generales sobre la valoración de la autenticidad de un documento electrónico, puesto que los DVD aportados a un proceso penal por agentes de policía no pueden aspirar a un régimen privilegiado frente a la autenticidad afirmable de esos mismos soportes electrónicos cuando tienen distinto origen.

Recuerdan los autores del voto particular, que el artículo 115 de la Ley 24/2001, 27 de diciembre, que dio nueva redacción al artículo 17 bis de la más que centenaria Ley del Notariado, fechada el 28 de mayo de 1862, en su apartado 3, se regula la garantía que ha de reunir una copia notarial para estimar acreditada su autenticidad. En él se dispone: "[…] *las copias autorizadas de las matrices podrán expedirse y remitirse electrónicamente, con firma electrónica avanzada, por el notario autorizante de la matriz o por quien le sustituya legalmente",* pero las garantías asociadas a los archivos y documentos electrónicos, no son exclusivas del trabajo desplegado por los Notarios. La propia Administración impone semejantes requerimientos técnicos de autenticidad, cuando es el ciudadano el que se relaciona con los órganos administrativos. En efecto, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, ha querido definir las condiciones para que la actividad administrativa y las relaciones de los poderes públicos con los ciudadanos puedan ajustarse a las nuevas tecnologías. Ese ambicioso proyecto, orientado a la creación de una

genuina *Administración Electrónica,* no ha pasado por alto las exigencias de autenticidad. Así, en su artículo 13, bajo el epígrafe "*formas de identificación y autenticación",* se establece un principio general, referido a la admisibilidad de sistemas de firma electrónica, que luego es objeto de concreción. En el apartado 1 de ese precepto se dispone que "*…las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos".* Y añade el apartado 2 que *"…los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine: a) en todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas; b) sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas; c) otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen".*

Definidas las garantías de autenticidad exigibles a los ciudadanos, el mismo precepto, en su apartado 3, se refiere a idéntico tema desde la perspectiva de la propia Administración. En él puede leerse: *"las*

Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan: a) sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras; b) sistemas de firma electrónica para la actuación administrativa automatizada; c) Firma electrónica del personal al servicio de las Administraciones Públicas; d) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes..".

Estas garantías han sido objeto de desarrollo en el Real Decreto 1671/2009, 6 de noviembre, cuyo Preámbulo recuerda que, en materia de identificación y autenticación, se impone como medio universal la utilización de dispositivos de firma electrónica, sin perjuicio de otros medios de autenticación que cumplan con las condiciones de seguridad y certeza necesarias.

Es comprensible que el Ministerio de Justicia no haya permanecido al margen de esa preocupación legislativa tendente a asegurar la autenticidad de los ficheros electrónicos. Así, se desprende, por ejemplo, de la Orden Ministerial 3000/2009, 29 de octubre, por la que se crea y regula el Registro Electrónico del Ministerio de Justicia. En su artículo 9.1 se dispone que *"... los escritos, solicitudes y comunicaciones remitidos por medios electrónicos exigirán la identificación de los interesados*

remitentes y podrán firmarse mediante: a) los sistemas de identificación y firma electrónica incorporados al documento nacional de identidad para personas físicas; b) los sistemas de firma electrónica avanzada y firma electrónica reconocida ; c) las claves concertadas previo registro como usuario, la información conocida por ambas partes u otros sistemas no criptográficos, en los términos que especifiquen las instrucciones de acceso y utilización del Registro Electrónico en cada procedimiento disponible en la sede electrónica del departamento".

Aluden, asimismo, a que el legislador, hacía apenas dos meses, había abordado la regulación de la documentación de los debates del juicio oral y a que lo hizo con ocasión de la promulgación de la Ley 13/2009, 3 de noviembre, de reforma de la legislación procesal para la implantación de la nueva Oficina judicial, y ha proyectado sus previsiones sobre todos los órdenes jurisdiccionales (artículos 453 de la LOPJ, 743 de la Ley de Enjuiciamiento Criminal, 147 de la Ley de Enjuiciamiento Civil, 89.2 Ley de Procedimiento Laboral y 63.4 Ley de Jurisdicción Contencioso-administrativa).

La filosofía que inspira dicha reforma, en este concreto aspecto, guarda un saludable equilibrio entre el deseo político de implantación de nuevos modelos de gestión procesal y el realismo que impone el desfase tecnológico de nuestros Juzgados y Tribunales y, precisamente por ello, ha impuesto el deber de grabación de las sesiones del juicio oral en un soporte técnico que sea apto para la reproducción del sonido y la imagen.

Al mismo tiempo, ha recordado el deber de custodia que incumbe al Secretario Judicial (Letrado de la Administración de Justicia) respecto de esos soportes. La norma abre la puerta a la utilización de documentos electrónicos cuyo contenido pueda ser adverado mediante firma electrónica. De su utilización que, como es lógico, estará condicionada a su efectiva disponibilidad en la oficina judicial, se hace depender, tanto la necesidad de presencia real del Letrado de la Administración de Justicia en las sesiones del juicio, como las menciones que ha de recoger el acta. La razón es bien clara y se desprende del mismo precepto: sólo en el caso en que el documento esté garantizado con firma electrónica estará a salvo su integridad y autenticidad. Repárese, además, que en el presente caso de lo que se trata es de un documento al que se incorpora un archivo de sonido o imagen que ha sido generado durante el transcurso de un acto procesal, presidido por un órgano jurisdiccional y con la garantía añadida de la custodia formal del fedatario judicial.

En definitiva, el establecimiento de un sistema que garantice, cuando menos, la integridad de cualquier documento electrónico, constituye un *prius* para la atribución al mismo de plena eficacia probatoria. Así lo ha entendido el legislador español, en sintonía con un imparable proceso de unificación en el ámbito de la Unión Europea, requiriendo esas garantías, incluso cuando el documento emana de un fedatario público.

En el aspecto normativo, también se combate la resolución judicial mayoritaria, recordando que las normas jurídicas que regulan el funcionamiento del sistema integrado de interceptación telefónica son básicamente dos. Una de ellas, el Real Decreto 424/2005, 15 de abril, buena parte de cuyo contenido fue incorporado al artículo 33 de la Ley 32/2003, 3 de noviembre, General de las Comunicaciones, en virtud de la reforma operada por la Disposición Final 1ª de la Ley 25/2007, 18 de octubre, sobre conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Esta norma ha de ser completada con la Orden ITC/110/2009, 28 de enero, por la que se determinan los requisitos y las especificaciones técnicas que resultan necesarios para el desarrollo del Capítulo II del Título V del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, 15 de abril.

Pues bien, la lectura detenida de ambos textos normativos (en especial, de este último, que fija los requerimientos técnicos exigibles para la ejecución de la orden judicial de interceptación), pone de manifiesto que todas las garantías y reservas que el sistema incorpora, *sólo miran a la relación entre los agentes de policía facultados y las operadoras de telefonía*. La citada OM 110/2009 contempla la necesidad de crear lo que denomina "*…bloques funcionales o interfaces del sistema de interceptación legal",* y arbitra varios canales seguros y resuelve los niveles de seguridad exigibles en la dirección bilateral que ha de

establecerse entre la Policía y las operadoras para la gestión de la orden judicial de injerencia.

El problema radica en que todo ese sistema de controles y garantías se arrincona cuando los agentes facultados vuelcan en un DVD las conversaciones que estiman más relevantes y se presentan ante el Juzgado, mediante una comparecencia personal, aportando un soporte electrónico con vocación de *originalidad*[218]. Éste es el problema de origen que impide a estos magistrados avalar el funcionamiento del sistema integrado (SITEL) que, si bien se mira, no lleva su *vocación integradora* hasta sus últimas consecuencias, pues se olvida de integrar a los órganos jurisdiccionales en el esquema que define su funcionamiento.

El voto particular critica que la interceptación de las comunicaciones telefónicas, con arreglo a las sofisticadas posibilidades que ofrece cualquier sistema integrado, no debería haber prescindido de una idea tan elemental como la existencia de tres sujetos funcionales distintos: a) las operadoras de telefonía -sujetos obligados-, b) los

[218] Voto particular formulado por D. Manuel Marchena, al que se adhiere D. José Manuel Maza, pronunciado en sentencia, Sala Segunda, del Tribunal Supremo 1215/2009, de 30 de diciembre, apartado III :*"[…] En ese instante, los canales seguros y las interfaces que la Orden ITC/110/2009 impone a operadoras y agentes facultados, dejan paso a un incontrolado volcado de datos que, lejos de ser transmitidos por vía telemática, se presentan ante el Juzgado de instrucción por un agente de policía que afirma haber seleccionado aquellos fragmentos que considera relevantes para la investigación.*

[…]Este último dato, por cierto, nos debe hacer pensar en la paradoja que encierra el hecho de que la transmisión de información entre los operadores de telefonía y los agentes facultados de las Fuerzas y Cuerpos de Seguridad del Estado, se verifique con la exigencia de firma electrónica. Sin embargo, en el momento decisivo de su incorporación al proceso penal, para su valoración como fuente de prueba, la relación del órgano jurisdiccional con esos mismos agentes, recupera el añejo sabor artesanal de las comparecencias personales, aportando un documento cuyo contenido ha de ser acatado sin cuestionar su integridad".

funcionarios de policía -agentes facultados- y c) los Jueces de Instrucción que autorizan la interceptación y que se convierten en destinatarios últimos del resultado de las escuchas. Así, si bien las normas reguladoras del SITEL han diseñado un sistema de garantías en las relaciones entre dos de aquellos sujetos, operadoras y policía, no han previsto, de forma incomprensible, el momento de la incorporación de las pruebas electrónicas generadas al proceso penal. En ese instante, los canales seguros y las interfaces que la Orden ITC/110/2009 impone a operadoras y agentes facultados, dejan paso a un incontrolado volcado de datos que, lejos de ser transmitidos por vía telemática, se presentan ante el Juzgado de Instrucción por un agente de policía que afirma haber seleccionado aquellos fragmentos que considera relevantes para la investigación.

La preocupación por una seguridad integral, que no admita grietas en alguno de los pilares sobre los que opera el sistema, está bien presente en la Exposición de Motivos del Real Decreto 3/2010, 8 de enero, por el que se regula el *Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*. La limitación de su ámbito aplicativo no resta valor a algunos de los pasajes de la Exposición de Motivos. Ahí puede leerse que "*…la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Es por ello que cada sistema debe tener claro su perímetro y los responsables de cada dominio de seguridad deben coordinarse efectivamente para evitar «tierras de nadie» y fracturas que pudieran dañar a la información o a los servicios prestados.*

Insiste el texto en la necesidad de huir de una concepción parcelada y fragmentaria de la seguridad informática: —…se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas".

El SITEL, en fin, convierte a los Juzgados y Tribunales en un *punto débil,* en una *tierra de nadie* en la que las garantías de seguridad e integridad del documento electrónico se degradan de forma insalvable. Los Jueces de Instrucción se transforman, así, *en meros receptores de unos soportes electrónicos cuyo contenido no puede apoyarse en otra garantía que la confianza acrítica en la profesionalidad de los agentes que se los proporcionan*. Y tal sistema de operar provoca que el Letrado de la Administración de Justicia, en su condición de fedatario, se vea obligado a suscribir un acto de adveración a ciegas, no pudiendo dar fe de que el contenido de esos DVD coincide con un original al que no tiene acceso, pues la oficina judicial ha sido excluida de cualquier interfaz que permita el seguimiento de las interceptaciones, no pudiendo garantizar que no se han eliminado erróneamente fragmentos de conversaciones de indudable trascendencia jurídica y que, sin embargo, han podido ser excluidos en el momento del volcado al soporte electrónico. Dicho de forma bien gráfica, el Secretario sólo podrá adverar que el DVD presentado por la Policía es efectivamente el que presenta la Policía.

De ahí que no compartan el criterio mayoritario, expresado en el FJ 17 de la sentencia, cuando sostiene que "…*el sistema de escuchas telefónicas, que se plasma en un documento oficial obtenido con autorización judicial y autenticado su contenido por la fe pública judicial goza de valor probatorio, salvo que mediante pericia contradictoria se demuestre la falsedad o alteración de las conversaciones grabadas".*

A tenor de la opinión de los magistrados que suscribieron el voto particular, los soportes digitales aportados por los agentes, como toda prueba electrónica, deben pasar por un test de admisibilidad y éste comprende el análisis de su integridad (esto es, que el soporte no ha sido alterado), de su autenticidad (o sea, la identificación del sujeto al que se atribuyen las conversaciones) y del contenido que éstas reflejan, y por último, de su licitud, es decir, de que han sido obtenidos con respeto a los derechos y libertades fundamentales.

En este caso, y en relación al documento electrónico consistente en varios DVD en los que se incorporan archivos digitales de sonido, la valoración jurisdiccional exige dos niveles de autenticidad, así:

1º El que garantiza que, una vez grabada la conversación en el terminal custodiado por los agentes de policía, el fichero así generado no ha sido abierto con posterioridad y, en consecuencia, no ha sido expuesto a ningún tipo de modificación. El Tribunal que

ha de valorar esa fuente probatoria ha de tener asegurado, en el plano tecnológico, que no se han suprimido fragmentos relevantes para conocer el alcance de los hechos o que no han sido excluidas conversaciones que el agente responsable considera intrascendentes jurídicamente y que, sin embargo, pueden no serlo. En definitiva, resulta indispensable que el sistema garantice que, después de cada conversación interceptada por los agentes facultados, se procede al sellado tecnológico del archivo de sonido, con el fin de salvaguardar su integridad, excluyendo cualquier riesgo de manipulación. Si, como es lógico y previsible, esos archivos han de ser abiertos durante el desarrollo de la investigación, el sistema podría completarse con la intervención de un tercero ajeno al agente responsable, que encontrara inspiración en los términos del artículo 25 de la Ley 34/2002, 11 de julio , de Servicios de la Sociedad de Información y del Comercio Electrónico, sin descartar la posibilidad de que ese sellado pudiera verificarse a través de una interfaz que conectará al Letrado de la Administración de Justicia con el centro de operaciones, garantizándose, así, una matriz de prueba frente a posibles y futuras impugnaciones.

2º Teniendo presente que la fuente de prueba ofrecida por los agentes de policía a la valoración del Tribunal está integrada, no por los ordenadores centrales, sino por las copias incorporadas a uno o varios DVD, se impone, en consecuencia, un segundo nivel

de exigencia, que ahora afecta al soporte en el que se incorpora la copia de los archivos originales. De ahí, que resulte indispensable que, inmediatamente después de efectuado el proceso de grabación, se active una certificación que garantice: a) que desde el momento en que culminó el proceso de transferencia de archivos hasta su recepción por el Juzgado, ese DVD no ha sido abierto, b) que, en consecuencia, no ha existido riesgo de manipulación y c) que quien garantiza la integridad del documento es el funcionario responsable del tratamiento y, por tanto, el único con capacidad de autentificación.

Sostienen los magistrados, que la secuencia grabación-copia-incorporación al proceso se culmina con una simple comparecencia personal, sin filtro alguno que garantice la integridad y autenticidad de los soportes. Este dato, a su juicio, es obviado por el criterio de la mayoría, que concluye la autenticidad de los DVD a partir de un análisis incompleto de lo que deben ser las exigencias de seguridad e integridad. Enfatizan que el acceso por parte del personal de la unidad de policía se realiza *"... mediante identificador de usuario y clave personal"*, y entienden no añade nada a la solución del problema que nos ocupa. En efecto, esta idea, desarrollada en el razonamiento incorporado al FJ 14, obliga a una importante puntualización. En él puede leerse: *"... se ha dicho que estos discos, dadas las características de la tecnología digital, pueden ser alterados mediante sofisticadas operaciones de laboratorio. Esta objeción no se descarta, ahora bien, así como en el antiguo sistema de*

manipulación, los cortes eran posibles sin saber de forma cierta quién los había realizado materialmente, en el sistema SITEL se deja huella identificadora del manipulador ya que debe facilitar su clave de identificación para entrar en el disco duro. En este caso, nos encontraríamos ante un delito que de confirmarse su existencia a posteriori podría dar lugar a la revisión de la sentencia". En su opinión, el control jurisdiccional de las garantías procesales no puede contentarse con la tranquilidad que proporciona que, de producirse una manipulación, la impunidad no estaría garantizada, o con la idea de que siempre habrá tiempo para un ulterior juicio de revisión. Las garantías, entienden, deben ser inmanentes al sistema, sin que su afirmación pueda quedar postergada a un momento ulterior, una vez detectada su vulneración.

a.2.3.- Jurisprudencia y doctrina posterior

La Sala Segunda ha ratificado, posteriormente, este sistema (SITEL), entre otras, en la Sentencia del Tribunal Supremo, Sala Segunda, 327/2010, de 12 de abril, en donde se concluye: *"y en suma, la legalidad de la medida, la audición, la aportación de los CD, y los criterios de interceptación, han sido realizados conforme a lo autorizado en la doctrina resultante de la STS 1215/2009, de 30 de diciembre (sistema SITEL)"*, y en la sentencia del Tribunal Supremo, Sala Segunda, 554/2012, de 4 de julio, donde se explica cómo los usuarios del sistema, los grupos operativos encargados de la investigación, no acceden en ningún momento al sistema central de almacenamiento, recogiendo

únicamente un volcado de esa información con la correspondiente firma electrónica digital asociada, transfiriéndola a un CD o DVD para su entrega a la Autoridad judicial, garantizando de esta manera la autenticidad e integridad de la información almacenada en el sistema central[219].

El TS señala que la posibilidad de manipulación o alteración del resultado de las intervenciones en el sistema SITEL es prácticamente imposible (sentencia del Tribunal Supremo, Sala Segunda, 410/2012, de 17 de mayo) pues se trata de un *"…sistema de grabación de alta seguridad…con mayor seguridad que en un sistema tradicional de cintas analógicas".* Es un sistema *"…preferible a los modos de intervención anteriores a su implantación…"* (Sentencia del Tribunal Supremo, Sala Segunda, 1078/2009, 5 de noviembre).

La posición dominante se ha dejado seducir por las garantías de seguridad que muestra SITEL, lo que le ha permitido establecer un auténtico principio de presunción de autenticidad que, sin duda, ha

[219] Se valora como garantía adicional, la escisión funcional entre policías que escuchan y policías que investigan *"de manera que el órgano policial de investigación recibe lo que otro órgano ha grabado de acuerdo al sistema de interceptación. Esa distinción entre órganos de investigación e interceptación evita riesgos de alteración de sus contenidos que pudieran plantearse dado el desconocimiento por el órgano de escucha del objeto de la investigación. También, la propia digitalización de la interceptación permite asegurar que cualquier hipotética manipulación dejará rastro de su realización, lo que, en principio, se evita mediante la fijación horaria, haciendo imposible su manipulación…"* Sentencia del Tribunal Supremo, Sala Segunda, 629/2011, de 23 de junio.

conllevado la confirmación por la jurisprudencia[220] de la legitimidad de la utilización probatoria de las conversaciones grabadas por el sistema.

Aun a pesar de ello, no podemos dejar de mencionar que la posición antagónica ha vuelto a reproducirse en un nuevo voto particular, en este caso a la sentencia del Tribunal Supremo, Sala Segunda, 722/2012, de 2 de octubre, partiendo esencialmente de los mismos argumentos expuestos en su precedente del voto particular a la sentencia del Tribunal Supremo, Sala Segunda, 1215/2009, de 30 de diciembre. El voto particular estima en síntesis que sostener como principio la eficacia probatoria de los DVD generados por el sistema SITEL supone un retroceso respecto del estado actual de las garantías constitucionales y que la pertinencia de la impugnación dependerá siempre de las circunstancias concurrentes en el caso concreto, de los términos en que la propuesta probatoria haya sido formalizada, del objetivo que con ella se persiga y, en fin, de su necesidad para excluir dudas fundadas acerca de la integridad de los soportes.

Como bien dice la Circular 1/2013 de la Fiscalía General del Estado, desde un equipo remoto no es posible modificar ni borrar absolutamente nada del servidor central del SITEL. El contenido de las conversaciones y datos asociados queda íntegramente grabado en el

[220] Sentencias del Tribunal Supremo, Sala Segunda, 410/2012, de 17 de mayo, 250/2009 de 13 de marzo, 308/2009 de 23 de marzo, 1078/2009 de 5 de noviembre, 1215/2009 de 30 de diciembre, 740/2010 de 6 de julio, 753/2010 de 19 de julio, 764/2010 de 15 de julio, 293/2011 de 14 de abril, 565/2011 de 6 de junio, 419/2009, de 5 de noviembre; 629/2011, de 23 de junio, y 554/2012, de 4 de julio.

Servidor Central del SITEL, y no es posible su borrado sin autorización judicial específica, sin que sea posible su alteración porque queda registrado en el sistema cualquier intento de manipulación y ello de forma indeleble[221]. En cualquier momento del proceso es posible la verificación de la integridad de los contenidos volcados a los soportes CD/DVD entregados en el Juzgado, mediante su contraste con los que quedan registrados en el Servidor Central del SITEL, a disposición de la autoridad judicial, garantizando así la legalidad.

MARCHENA GÓMEZ[222] menciona críticamente esta Circular por ser el reflejo de una línea jurisprudencial que practica la incondicional confianza en las excelencias del actual sistema integrado de telefonía, y que, según su opinión, debería dejar paso a debería ir dejando paso a jurisprudencia más cautelosa, a la vista de los valores en juego.

Más adelante, la sentencia del Tribunal Supremo, Sala Segunda, 143/2013, de 28 de febrero, intentó ir más allá trayendo a colación al RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento que desarrolla la Ley de Protección de Datos (RPDCP), que, entre otras cosas, garantiza la inalterabilidad de la información almacenada, así como un efectivo y riguroso control de los accesos que se han producido a aquella,

[221] *"Los Tribunales en las causas en las que se haya procedido a la realización de intervenciones telefónicas, deberán acordar de oficio en sus sentencias la destrucción de las grabaciones originales que existan en la unidad central del sistema SITEL y de todas las copias, conservando solamente de forma segura las entregadas a la autoridad judicial, y verificando en ejecución de sentencia, una vez firme, que tal destrucción se ha producido"* Sentencia del Tribunal Supremo, Sala Segunda, 565/2011, de 6 de junio.

[222] MARCHENA GÓMEZ, M., *Proceso penal: nuevos problemas…, op. cit.*

nivel de seguridad que la resolución del Alto Tribunal asegura existe y está garantizado en el sistema SITEL.

Este cumplimiento de las más esenciales garantías es defendido por autores tales como GARCÍA-GALÁN SANMIGUEL[223] o RODRÍGUEZ LAÍNZ[224]. Este último enumera otra serie de cualidades del sistema, conocidas fruto de su experiencia profesional:

- Figura del coordinador de centros de recepción[225] , quien asegura que no se intercepten ni más terminales ni por más tiempo y objeto que los pautados en la resolución habilitante, siguiendo para ello un procedimiento sencillo y eficaz. El coordinador accede al contenido de la solicitud de conexión del sistema de interceptación remitido previamente al centro de interceptación por el agente

[223] GARCÍA-GALÁN SANMIGUEL, M. J., *La interceptación de las comunicaciones y su eficacia en el proceso penal*, en "Interceptación de las comunicaciones y nuevas tecnologías", Cuadernos Digitales de Formación, núm. 43, Consejo General del Poder Judicial, 2010, p. 2-3

[224] RODRÍGUEZ LAÍNZ, J. L., *SITEL: nuevas tendencias, nuevos retos*, Diario La Ley, núm. 8082, Sección Doctrina, Año XXXIV, Editorial LA LEY, 14 mayo de 2013.

[225] La figura del coordinador de centros de recepción viene regulada en la Orden ITC/110/2009, de 28 de enero, por la que se determinan los requisitos y las especificaciones técnicas que resultan necesarios para el desarrollo del capítulo II del título V del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril (BOE 29/2009, de 3 de febrero de 2009) —ORLGT—. En la relación de definiciones que se desarrollan en el anexo de dicha norma, se define al coordinador de centros de recepción como «persona o grupo de personas perteneciente a cada uno de los agentes facultados que será el único enlace válido para los sujetos obligados a los efectos de tratar asuntos relacionados con la interceptación legal de las comunicaciones». La finalidad de éste no es otra que la de actuar como interlocutor fiable para una serie de cometidos relacionados con la mejora y agilidad en la prestación del servicio o resolución inmediata de vicisitudes o incidencias; así: el coordinador del centro de recepción actúa como interlocutor en el canal no seguro de comunicación con los centros de interceptación —artículo 6.2,c)—; como punto de contacto para asegurar el plazo de inicio de una interceptación de comunicaciones fuera del horario laboral —artículo 8.2,3)—, o para servir de contacto para la solución de asuntos urgentes —artículo 9.6—. Realmente el coordinador actúa al servicio del agente facultado, como un delegado de éste.

facultado y a través de un canal seguro. Con ello y con la copia de la resolución, mandamiento u oficio emitidos por el Juzgado, que le son también proporcionados, coteja los datos grabados con el contenido de la resolución habilitante, minimizando el riesgo de errores en la trasposición de la orden de interceptación, por parte de la unidad policial a la que se ha encomendado tal cometido y, por ende, el riesgo de realizar intervenciones a terminales erróneos o por tiempo o alcances diversos a los realmente autorizados.

- La carpeta generada para cada interceptación, a la que se dota para ello de un número de identificación, va almacenando datos y contenidos (voz y mensajes SMS), generando automáticamente, a cada paso, una firma electrónica que garantiza ese primer nivel de actuación. Esta firma electrónica supone una garantía de que ese fichero, alojado en la concreta carpeta del centro de recepción, ha tenido lugar y de que su contenido es el que se refleja, sin que haya posibilidad de selección; a excepción de averías del sistema que puedan afectar a determinadas franjas horarias o concretas comunicaciones, todas y cada una de las comunicaciones que emita o reciba el terminal intervenido se almacenarán en la correspondiente carpeta.

- Los agentes facultados tienen, efectivamente, la capacidad de acceder a la carpeta donde se almacena la información de la interceptación en los archivos del centro de recepción, y de

examinar y oír los datos y archivos de audio que consideren oportunos; estando esos archivos protegidos frente a cualquier tipo de manipulación, en modo de "solo lectura"[226]. Utilizan, para ello, sus correspondientes códigos identificadores de usuario y claves personales y, a través de tal acceso, pueden incluso trabajar oyendo las conversaciones, transcribiéndolas o situando al usuario del terminal, prácticamente en tiempo real, en una ubicación geográfica determinada.

- El sistema de seguridad de SITEL asegura que todo acceso deje un registro, rastro, que puede ser analizado, auditado, a posteriori; lo cual reporta una mayor garantía sobre la inalterabilidad a este nivel.

VALLÉS[227] también defiende este sistema, planteando que su resultado es producto de una actividad policial que evoca el concepto de la prueba pericial de inteligencia o prueba de inteligencia policial. Propone el autor, como solución a la polémica, además de la revisión del concepto de evidencia digital que aporte seguridad jurídica al acto de su incorporación al proceso penal, el incorporar, cuanto antes, sistemas de salvaguarda y certificación que desplacen los debates procesales a su

[226] Sentencias del Tribunal Supremo, Sala Segunda, entre otras, 308/2009, de 23 de marzo, 1215/2009, de 30 diciembre, 740/2010, de 6 de julio, 753/2010, de 19 de julio, 764/2010, de 15 de julio, 293/2011, de 14 de abril, 565/2011, de 6 de junio, 554/2012, de 4 de julio, y 722/2012, de 2 de octubre.

[227] VALLÉS CAUSADA, L. M., "La policía judicial en la obtención de inteligencia…", *op. cit.*, p.375.

lugar natural, o valoración de la prueba durante el acto del juicio oral y, en ningún caso, al medio técnico con que se obtuvo.

Por el contrario, otros autores, entre los que ponemos como ejemplo al magistrado del Tribunal Supremo MARCHENA GÓMEZ[228], continúan ofreciendo una visión crítica. Así, para él, reproduciendo el contenido de su voto particular a la Sentencia 1215/2009, reitera que no existen razones jurídicas que justifiquen que el resultado de los actos de investigación encomendados a las Fuerzas y Cuerpos de Seguridad del Estado se sustraiga a las reglas generales sobre la valoración de la autenticidad de un documento electrónico. Los DVD aportados a un proceso penal por agentes de policía no pueden aspirar a un régimen privilegiado frente a la autenticidad afirmable de esos mismos soportes electrónicos cuando tienen distinto origen. Dicho con otras palabras, el DVD, aportado por los agentes, no puede gozar de una autenticidad, irrazonablemente aventajada, frente al DVD en el que se contienen, por ejemplo, escrituras públicas y está custodiado por un Notario[229].

Por el contrario, GONZÁLEZ LÓPEZ[230] defiende que los soportes digitales aportados por los agentes, como toda prueba electrónica, han de

[228] MARCHENA GÓMEZ, M., *Proceso penal: nuevos problemas… op. cit.*

[229] Artículo 115 de la Ley 24/2001, de 27 de diciembre, que dio nueva redacción al artículo 17 bis de la Ley del Notariado de 28 de mayo de 1862.

[230] GONZÁLEZ LÓPEZ, J. J., *Intervención de las comunicaciones: Nuevos desafíos, nuevos límites*, en PÉREZ GIL, J. (Dtor.) "El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito", Editorial LA LEY, Madrid, 2012, p. 110-115.

pasar por un test de admisibilidad que comprende tres aspectos, satisfechos, según él, por el sistema SITEL:

a) El análisis de su integridad, es decir, que el soporte no haya sido alterado una vez grabada de información en el terminal custodiado por los agentes.
b) El análisis de su autenticidad o la identificación del sujeto al que se le atribuyen las conversaciones y el contenido que éstas reflejan.
c) El estudio de su licitud, es decir, que la obtención de datos haya sido realizada con respeto a los derechos y libertades fundamentales.

Por último, la sentencia del Tribunal Supremo, Sala Segunda, 849/2013, de 12 de noviembre, soluciona cuestiones tales como la posible falta de autenticidad del contenido de los CD y su posible manipulación, exponiendo, tras recordar sentencias anteriores, que al sistema SITEL (el cual vierte la información en discos ópticos de gran capacidad con datos de un gran número de interceptaciones y que, por sus características técnicas, a la información que contienen dichos discos sólo se puede acceder si están conectados al sistema central y únicamente a través de éste) se le implantó un sistema de firma desasistida y que asocia a cada archivo que se produce en SITEL un archivo de firma que garantiza que el archivo a comprobar no se ha modificado, ni en un solo bit, desde el momento en que se grabó en

SITEL, tanto si se hace la comprobación en el sistema central, como si se hace en los CD o DVD en los que se vuelca la información para su entrega a la autoridad judicial.

SITEL utiliza una aplicación de firma electrónica que almacena la información referente a la firma y al certificado del prestador de servicios de certificación como metadatos en los documentos electrónicos. Se realiza mediante un servicio de sellado documental automatizado y desasistido, con uso de un certificado digital de la empresa Camerfirma S.A.[231].

Todo lo anterior es acorde al nuevo contenido de la Ley de Enjuiciamiento Criminal, así artículo 588 ter f, cuando al respecto del *control de la medida*, y en relación a la interceptación de las comunicaciones, dispone que *"[…] se asegurará, mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas"*, por lo que, desde el punto de vista técnico, nada podemos objetar al sistema SITEL.

[231] Empresa reconocida para la emisión de certificados a las Administraciones Públicas en base al desarrollo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. La validez de este sistema de certificado y la eficacia probatoria de los archivos creados por el sistema de interceptación ha sido reconocida por el Tribunal Supremo, Sala Segunda, en sentencias como la 554/2012.

b) GOLF

GOLF[232] surgió como un sistema de interceptación de las comunicaciones de voz. En el año 2000 se adquiere el primer modelo GOLF 7.9, datando sus primeras interceptaciones en el mes de septiembre del año 2001. En sus comienzos, era capaz de interceptar telefonía fija y móvil analógica. Sin embargo, con el paso de los años y debido a las crecientes necesidades del servicio, el sistema se fue mejorando y ya en el año 2006 comienzan a interceptarse Internet (paquetes de datos) y líneas RDSI, dando el salto a la comunicación digital.

Es en el año 2008 cuando se produce el cambio más trascendental del sistema, con la llegada de GOLF 10.1 que permitió desde entonces integrar las sondas tácticas de interceptación al sistema.

Actualmente, el sistema GOLF permite la interceptación de telefonía móvil (GSM, GPRS, UMTS), fija, paquetes de datos de Internet, mensajería instantánea como el *WhatsApp*[233], fax, e intervenciones especiales (sondas tácticas).

[232] El nombre completo del programa es GOLF RELIANT debido a la empresa que lo fabricó VERINT RELIANT, aunque comúnmente se denomina simplemente GOLF.

[233] A partir de la versión 2.8.3. de *WhatsApp*, esta aplicación de mensajería, aunque puede ser interceptada, no muestra los datos en claro debido al cifrado de sus mensajes.

GOLF comparte red con el sistema SITEL, de modo que utiliza el mismo puesto de telecomunicaciones que es usado para la intervención de las comunicaciones mediante SITEL, pero no interfiere en el funcionamiento del mismo. Ambos sistemas pueden coexistir al mismo tiempo sin que se vea afectado el trabajo de los operadores.

Para el acceso a la aplicación, es necesario contar con un usuario y una contraseña. Al tratarse de una aplicación web, el acceso ha de realizarse a través de Internet, accediendo al servidor *citrix*[234].

Una vez se ha accedido a *citrix*, este muestra uno o varios accesos directos, debiéndose introducir un nuevo usuario y contraseña en la aplicación WWS. Es entonces cuando ya se puede visualizar las comunicaciones intervenidas, ya sean telefónicas, fax, chats y mensajería instantánea, navegación por Internet etc., lográndose, incluso, la intervención y observación o escucha en tiempo real de todas ellas.

A la vista de su configuración técnica, entendemos que a este sistema también le sería de aplicación todo lo expuesto en torno a la legalidad del SITEL.

c) SILC

[234] El primer acceso se realiza a través de un control remoto desde el centro de monitorización ubicado en Madrid, requiriendo únicamente el código IP del ordenador a usar.

La empresa DARS se crea en el 2007 entre las empresas RCS (italiana) y DATATRONICS (española) e inicialmente se dedicaba a la colocación de sondas tácticas de varias tecnologías. En su evolución introduce en el mercado un sistema de interceptación de las telecomunicaciones denominado SILC, el cual es adquirido por la Policía Foral de Navarra.

En el 2011, la Guardia Civil adquiere un compromiso con esta empresa, a través del Ministerio del Interior, para la colocación en su Centro de Monitorización de Barajas de un sistema integrado que permite, tanto intervenciones de telefonía tradicional y móvil, como de VoIP, permitiendo integrar las sondas tácticas de DARS, así como de otros proveedores.

Actualmente es el sistema de interceptación más avanzado en cuanto a la decodificación de los paquetes de datos interceptados de Internet.

Para poder tener acceso al sistema, los administradores se encargarán de dar de alta a aquellas personas que lo soliciten y estén autorizadas para ello. Se les designará un nombre de usuario y una contraseña, que deberán ser introducidas cada vez que se inicia una sesión.

Una vez el usuario ha sido autentificado, el sistema mostrará el programa que va a ser ejecutado, siendo necesario que el cliente cuente con Internet Explorer 8 y además, los instaladores del sistema tienen que configurar una serie de opciones para su correcto funcionamiento.

Una vez que se accede al sistema, el usuario puede ver solamente aquellos objetivos que tiene asignados, y muestra a los agentes autorizados una imagen muy similar a la que puede ver el objetivo interceptado, en el caso de paquetes de datos, mensajería instantánea como *WhatsApp* etc.

A este sistema le sería de aplicación todo lo expuesto en torno a la legalidad del SITEL.

I.3.- Especial referencia a las falsas estaciones BTS

El escrutinio de esta clase de información manejada a nivel técnico por las operadoras de comunicaciones electrónicas, para la prestación de su servicio, con el objetivo de descubrir quién estaba detrás de unas llamadas realizadas en el escenario de un crimen, fue precisamente empleado en el supuesto analizado por la sentencia del Tribunal Supremo, Sala Segunda, 777/2012, de 17 de octubre, que entendió que *"ninguna vulneración puede predicarse de la utilización de un método que lo único que pretende es conseguir, en un radio de acción prefijado, la activación de unos mecanismos de comunicación, traducidos en números,*

de donde pueda inferirse la localización de unos terminales de donde inducir la presencia de unos pocos sospechosos que respondan a la utilización más certera de un material que se ha conseguido por otros medios probatorios y que, como hemos visto, se han obtenido a través de informaciones directas, comprobables y legítimas".

Esta es precisamente la vía empleada por los aparatos de detección de números IMSI o IMEI utilizados por nuestras Fuerzas y Cuerpos de Seguridad[235], que generan o fuerzan un diálogo con el terminal en el que este se hace permeable a la falsa BTS.

Para RODRÍGUEZ LAÍNZ[236], estaríamos más cerca de la provocación de una comunicación electrónica automática (de la que el titular o usuario del terminal simplemente no es conocedor, ni menos partícipe voluntario), que de una simple captación. No es que, como afirma la sentencia del Tribunal Supremo, Sala Segunda, 430/2012, de 29 de mayo[237], la obtención del IMSI mediante procesos de monitorización no permita el acceso a números de teléfono en comunicación, sino que se actúa sobre unos ámbitos completamente ajenos a la voluntad del titular o usuario del terminal.

---

235 *"De unos años a esta parte, los departamentos de apoyo tecnológico de los diferentes cuerpos policiales se han ido dotando de medios técnicos para este fin, como sería el caso del IMSI Catcher o Interrogador de IMSI e IMEI, cuyos usos se extienden también a las funciones críticas de geolocalización de terminales de telefonía móvil".*

Vid., VALLÉS CAUSADA, L. M., "La policía judicial en la obtención de inteligencia…", *op. cit.*, p.352.

236 RODRÍGUEZ LAÍNZ, J. L., *Internet de los objetos…*, *op. cit.*

237 Sentencia del Tribunal Supremo, Sala Segunda, 430/2012, de 29 de mayo, FJ 2: "*En cuanto a la obtención policial de los IMEI o IMSI de algunos de los teléfonos, la doctrina de esta Sala es igualmente reiterada y conocida, y es citada correctamente en la sentencia impugnada. Por lo tanto, se entiende que no se ha afectado al derecho al secreto de las comunicaciones, ya que la obtención de tales datos no permite conocer los números de teléfono en comunicación".*

Para el autor anterior, la jurisprudencia del Tribunal Supremo no ha encontrado una solución plenamente satisfactoria al conflicto que se genera por razón del forzado de generación de diálogos entre terminal y falsa antena BTS, a través de los que el dispositivo policial al uso extrae información sobre número IMEI o IMSI; estos diálogos que, desde un punto de vista laxo, tendrían la naturaleza de auténticas comunicaciones. Entiende que, desde la que califica como meritoria y elaborada sentencia del Tribunal Supremo, Sala Segunda, 249/2008, de 20 de mayo[238], tales identificadores numéricos, que no alfanuméricos, no

[238] Sentencia del Tribunal Supremo, Sala Segunda, 249/2008, de 20 de mayo, FJ4: *"el concepto de datos externos manejado por el TEDH en la tantas veces invocada sentencia del Caso Malone, ha sido absolutamente desbordado por una noción más amplia, definida por la locución "datos de tráfico", en cuyo ámbito se incluyen elementos de una naturaleza y funcionalidad bien heterogénea. Y todo apunta a que la mecánica importación del régimen jurídico de aquellos datos a estos otros, puede conducir a un verdadero desenfoque del problema, incluyendo en el ámbito de la protección constitucional del derecho al secreto de las comunicaciones datos que merecen un tratamiento jurídico diferenciado, en la medida en que formarían parte, en su caso, del derecho a la protección de datos o, con la terminología de algún sector doctrinal, del derecho a la autodeterminación informativa (artículo 18.4 CE).*

C) Conforme a esta idea, la Sala no puede aceptar que la captura del IMSI por los agentes de la Guardia Civil haya implicado, sin más, como pretende el recurrente, una vulneración del derecho al secreto de las comunicaciones. No es objeto del presente recurso discernir, entre todos los datos de tráfico generados en el transcurso de una comunicación telefónica, cuáles de aquéllos merecen la protección reforzada que se dispensa en el art. 18.3 de la CE. En principio, ese carácter habría de predicarse, actualizando la pauta interpretativa ofrecida por el TEDH, de los datos indicativos del origen y del destino de la comunicación, del momento y duración de la misma y, por último, los referentes al volumen de la información transmitida y el tipo de comunicación entablada. Y la información albergada en la serie IMSI, desde luego, no participa de ninguna de esas características. Varias razonas avalan esta idea.

En primer lugar, que en los supuestos de telefonía móvil con tarjeta prepago esa información, por sí sola, no permite obtener la identidad de los comunicantes, la titularidad del teléfono móvil o cualesquiera otras circunstancias que lleven a conocer aspectos susceptibles de protección por la vía del derecho al secreto de las comunicaciones. En segundo lugar, que esa numeración puede llegar a aprehenderse, incluso, sin necesidad de que el proceso de comunicación se halle en curso. Con ello quiebran también las ideas de funcionalidad y accesoriedad, de importancia decisiva a la hora de calificar jurídicamente el alcance de la tutela constitucional de esa información.

D) Es evidente, sin embargo, que la negación del carácter de dato integrable en el contenido del derecho al secreto de las comunicaciones, no implica su irrelevancia constitucional. La información incorporada a la numeración IMSI es, sin duda alguna, un dato, en los términos de la legislación llamada a proteger la intimidad de los ciudadanos

participan de la naturaleza de datos de tráfico de una comunicación protegidos por el secreto de las comunicaciones, al no permitir desvelar por sí mismos la identidad del titular, por poderse obtener tal código sin necesidad de una concreta injerencia sobre una comunicación en curso, y no obedecer a los conceptos de funcionalidad y accesoriedad. Tampoco participan de esa naturaleza por no tratarse de unos datos mínimamente sensibles, que, por tanto, podrían ser captados y tratados por las Fuerzas y Cuerpos de Seguridad, aunque no de manera ilimitada o desproporcionada[239], sin necesidad de una previa autorización judicial, conforme a lo establecido en el artículo 22.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

frente a la utilización de la informática (art. 18.4 de la CE). Y es que, por más que esa clave alfanumérica, por sí sola, no revele sino una sucesión de números que ha de ser completada con otros datos en poder del operador de telefonía, su tratamiento automatizado haría posible un significativo nivel de injerencia en la privacidad del interesado. Que la numeración del IMSI encierra un dato de carácter personal es conclusión que se obtiene por la lectura del art. 3.a) de la LO 15/1999, 13 de diciembre, de Protección de Datos de Carácter Personal), con arreglo al cual, dato personal es "...cualquier información concerniente a personas físicas identificadas o identificables".

Siguen la misma tesis jurisprudencial resoluciones tales como las sentencias del Tribunal Supremo, Sala Segunda, 753/2010, de 19 de junio, 895/2010, de 14 de octubre, 79/2011, de 15 de febrero, 105/2011, de 23 de febrero, 185/2011, de 15 de marzo, 430/2012, de 29 de mayo, 478/2012, de 29 de mayo, y 676/2012, de 26 de julio.

[239] Sentencia del Tribunal Supremo, Sala Segunda, 676/2012, de 26 de julio: *"en aquel primer oficio policial, atestado de 25 de marzo de 2008, recoge el resumen de varios meses de investigación sobre algunos de los imputados, entre otras personas que finalmente no fueron objeto de acusación. En dicho informe se documenta la situación laboral y patrimonial de los mismos, con datos actualizados acompañados de los resultados de vigilancias y seguimientos, que corroboran tanto la escasa actividad laboral de los mismos (horarios, salidas...), como también la disposición de vehículos y propiedades, siendo en su mayoría personas que apenas han ejercido actividad laboral y teniendo en cuenta la edad de algunos de los imputados. Se solicitó la intervención de diez números de teléfonos y se autorizaron nueve. Es por ello que se aportaron datos concretos, que pudieron ser sometidos al juicio crítico del juez y que sirvió al instructor para concluir que los investigados podían estar dedicándose al tráfico de estupefacientes. El oficio está plagado de datos, fechas, horas y lugares, con expresa mención de los funcionarios partícipes de las vigilancias, ofreciéndose datos contrastables y contrastados, en la medida en que los funcionarios declararon en el juicio y ratificaron el resultado de las vigilancias.[…]Y las informaciones no se remiten a fuentes confidenciales, sino que son fruto del trabajo de investigación de la Guardia Civil, mediante vigilancias y seguimientos, sin que pueda sostenerse que la obtención de los números de teléfono no forme parte de esa investigación, alegando a inconcretas fuentes confidenciales, que no aparecen por ningún lado. En efecto, hay una laboriosa tarea policial de depuración.".*

Defiende el autor el carácter funcional del número IMSI en el desarrollo de la comunicación, desterrando de toda importancia al número de abonado por intrascendente[240], planteando cuestiones a reflexionar tales como lo contradictorio de llegar a comparar, como hace la STS, Sala Segunda, 791/2012, de 18 de octubre, un teléfono móvil con un domicilio a efectos de examen de su contenido, y sin embargo, se permita el acceso remoto a información en él contenida, como si se tratara de un intrascendente jurídico.

Con independencia de las valoraciones doctrinales al respecto, la Ley de Enjuiciamiento Criminal soluciona la problemática planteada. Por primera vez, tras la reforma experimentada gracias a 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, se recoge en su artículo 588 ter l la *identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes.*

Se regula la posibilidad de que los agentes de Policía Judicial puedan valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el

[240] RODRÍGUEZ LAÍNZ, J.L., *Dirección IP, IMSI e intervención judicial…*, *op. cit.*

equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.

Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de Policía Judicial pueden solicitar del Juez de Instrucción competente la intervención de las comunicaciones, debiendo poner en su conocimiento la utilización de los artificios usados. Tras ello, la autoridad judicial resolverá, de manera motivada, sobre la concesión o denegación de la solicitud de intervención conforme a los plazos legales.

Reconociendo la utilidad de esta regulación procesal que marca el camino a seguir por los investigadores, hemos de poner el punto de mira en la naturaleza de estos datos. Sabemos que es necesario una resolución judicial para la intervención de las comunicaciones cuyos datos de origen han sido obtenidos a través de falsas estaciones BTS, pero nada nos dice la norma al respecto de dichos datos.

De conformidad con todo lo expuesto, y ubicado el anterior precepto en la Sección 3ª, titulada *Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad*, no podemos considerarlos comunicación, por mucho que se esté forzando la comunicación entre dos dispositivos, el terminal móvil y la falsa antena BTS, y esto es así, porque ningún mensaje se transmite de manera voluntaria entre dos interlocutores. Aún es más, estando ante una

conexión (que no comunicación) generada entre dos artificios tecnológicos que arrastra como contenido identificadores numéricos, en todo caso, podríamos calificarlos como de "datos distintos a los de tráfico", sin perjuicio de que para su obtención sea necesaria autorización judicial.

I.4.- Medios tácticos de interceptación

Al igual que ocurre con las falsas estaciones BTS, los medios tácticos de interceptación en el aire de datos de tráfico precisan del empleo de medios técnicos tácticos adicionales a la propia red celular. Estos medios detectan y captan el tráfico IP de un dispositivo electrónico en la interfaz radio desplazándose a una zona próxima al mismo.

La obtención de la identificación y localización del equipo o del dispositivo de conectividad correspondiente o los datos de identificación personal del usuario, en relación con una IP, ha de cumplir las mismas exigencias ya vistas en cuanto a cesión de datos por las operadoras. Así, aparece regulado en la Ley de Enjuiciamiento Criminal, en su artículo 588 ter k.

De este modo, esta información estaría vinculada a la prestación de un servicio de comunicaciones electrónicas, y su captación, dejando a un lado a los operadores de las mismas, supondría la obtención de la misma fuera de los márgenes de ley, salvo que exista una autorización judicial

que habilite a los agentes de las Fuerzas y Cuerpos de Seguridad del Estado a emplear este método y lo podamos englobar en el artículo 588 ter l de la Ley de Enjuiciamiento Criminal.

II.- DATOS DE GEOLOCALIZACIÓN PROCEDENTES DE ESTACIONES DE BASE, WIFI Y GPS TRATADOS POR PRESTATARIOS DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

El marco jurídico pertinente es la Directiva sobre protección de datos (Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995)[241], que se aplica en todos los casos de tratamiento de datos personales, como resultado del tratamiento de datos de localización[242], quedando expresamente excluidos de la aplicación de la Directiva sobre la protección de la intimidad y las comunicaciones electrónicas, los datos de geolocalización obtenidos a través de los

[241] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[242] UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29, Dictamen 13/2011…, *op. cit.*

servicios de la sociedad de la información o empresas que ofrecen servicios de localización y aplicaciones basadas en una combinación de datos de estaciones de base, GPS y *WiFi*.

El ejemplo claro es cuando un usuario elige transmitir los datos GPS a través de Internet, accediendo a través de la red a servicios de navegación, siendo en ese caso la señal GPS transmitida independiente de la red GSM. El proveedor de servicios, aquí, es un mero transmisor, que no puede acceder, como regla general, a los datos GPS, *WiFi* o de estación de base comunicados desde y hacia un dispositivo móvil inteligente entre un usuario/abonado y un servicio de la sociedad de la información (la única excepción posible se da en el supuesto de la interceptación de las comunicaciones).

Esta Directiva busca como objetivo el hecho de que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, en lo relativo al tratamiento de dichos datos, sea equivalente en todos los Estados miembros.

A estos efectos, son "datos personales" toda información sobre una persona física identificada o identificable (el "interesado"); debiéndose considerar identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

El Dictamen 4/2007, del 20 de junio, sobre el concepto de datos personales, elaborado por el Grupo de Trabajo del artículo 29[243], que analiza esta materia, tiene como objetivo alcanzar un acuerdo sobre el concepto de datos personales y fijar los casos y manera en que debe aplicarse la legislación nacional sobre protección de datos.

Dicho Dictamen presenta el concepto de datos personales formado por cuatro componentes, los cuales están estrechamente ligados y se complementan recíprocamente:

1.- "Toda información" o todo tipo de afirmaciones sobre una persona abarcando tanto información "objetiva" (por ejemplo, la presencia de determinada sustancia en su sangre) como información "subjetiva", (opiniones o evaluaciones, sin que sea necesario que sean verídicas o estén probadas, de hecho, las normas de protección de datos prevén la posibilidad de que la información sea incorrecta y confieren al interesado el derecho de acceder a esa información y de refutarla a través de los medios apropiados). Asimismo está incluida la información relativa a la vida privada y familiar del individuo *stricto sensu*, pero también la información sobre cualquier tipo de activad desarrollada por una

[243] UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29, Dictamen 4/2007…, *op. cit.*

persona, como la referida a sus relaciones laborales o a su actividad económica o social.

Desde el punto de vista del formato o el soporte en que la información está contenida, el concepto de datos personales incluye la información disponible en cualquier forma, alfabética, numérica, gráfica, fotográfica o sonora, etc., así por ejemplo, la información conservada en papel, la almacenada en una memoria de ordenador, utilizando un código binario, o en una cinta de video.

2.- "Sobre": de modo general, se puede considerar que la información versa "sobre" una persona cuando se refiere a ella. Por ejemplo, los datos incluidos en el fichero personal de una persona guardado en el departamento de personal de su empresa están claramente relacionados con su situación, como empleado de dicha empresa.

A veces, no resulta tan clara la relación entre los datos y una determinada persona, por ejemplo cuando se refiere a objetos (objetos que pertenecen a alguien, están bajo la influencia de una persona o ejercen una influencia sobre ella o pueden tener una cierta proximidad física o geográfica con personas o con otros objetos).

Por tanto, para considerar que los datos versan "sobre" una persona debe haber un elemento "contenido" o un elemento "finalidad" o un elemento "resultado".

El elemento "contenido" está presente en aquellos casos en que - de acuerdo con lo que una sociedad suele general y vulgarmente entender por la palabra "sobre" – se proporciona información sobre una persona concreta, independientemente de cualquier propósito que puedan abrigar el responsable del tratamiento de los datos o un tercero, o de la repercusión de esa información en el interesado.

También la presencia de un elemento "finalidad" puede ser lo que determine que la información verse "sobre" determinada persona. Se puede considerar que ese elemento "finalidad" existe cuando los datos se utilizan o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona.

Existe una tercera categoría de "sobre" cuando existe un elemento de "resultado". A pesar de la ausencia de un elemento de "contenido" o de "finalidad" cabe considerar que los datos versan "sobre" una persona determinada porque, teniendo en cuenta todas las circunstancias que rodean el caso concreto, es probable que su uso repercuta en los derechos y los intereses de determinada

persona. Basta con que la persona pueda ser tratada de forma diferente por otros como consecuencia del tratamiento de tales datos[244].

3.- "Identificada o identificable". De modo general, se puede considerar "identificada" a una persona física cuando, dentro de un grupo de personas, se la "distingue" de todos los demás miembros del grupo. Por consiguiente, la persona física es "identificable" cuando, aunque no se la haya identificado todavía, sea posible hacerlo. La identificación se logra normalmente a través de datos concretos que podemos llamar "identificadores"[245] que tienen una relación privilegiada y muy cercana con una determinada persona, por ejemplo: altura, color del cabello, ropa, etc.

Al llegar a este punto, conviene señalar que, si bien la identificación a través del nombre y apellidos es, en la práctica, lo más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona. Así, puede suceder cuando se utilizan otros "identificadores" para singularizar a alguien, por ejemplo, en Internet, las herramientas de control de tráfico permiten identificar

[244] El Dictamen 4/2007, del 20 de junio, sobre el concepto de datos personales, elaborado por el Grupo de Trabajo del artículo 29, presenta, como ejemplo numerado con el 8, un sistema de localización de taxis para la optimización del servicio.

[245] La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, menciona esos "identificadores" en la definición de "datos personales" del artículo 2 cuando establece que "*se declarará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*".

con facilidad el comportamiento de una máquina y, por tanto, la del usuario que se encuentra detrás.

Más concretamente, y en lo relativo a las direcciones IP como datos sobre una persona identificable, el Dictamen 4/2007, del 20 de junio, sobre el concepto de datos personales, elaborado por el Grupo de Trabajo del artículo 29 ha declarado que "*los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva*"[246].

Especialmente en aquellos casos en los que el tratamiento de direcciones IP se lleva a cabo con objeto de identificar a los usuarios de un ordenador (por ejemplo, el realizado por los titulares de los derechos de autor para demandar a los usuarios por violación de los derechos de propiedad intelectual), el

[246] UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 DE LA DIRECTIVA 95/46/CE, Documento de trabajo *Privacidad en Internet: Enfoque comunitario de la protección de datos en línea*, de 21 de noviembre de 2000. Recuperado de: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37es.pdf (última consulta: 4 de junio de 2016).

responsable del tratamiento prevé que los "medios que pueden ser razonablemente utilizados" para identificar a las personas pueden obtenerse, por ejemplo, a través de los tribunales competentes (de otro modo, la recopilación de información no tiene ningún sentido) y, por lo tanto, la información debe considerarse como datos personales.

Un caso particular sería el de algunos tipos de direcciones IP que en determinadas circunstancias y por diversas razones técnicas y organizativas, no permiten realmente la identificación del usuario. Así sucede, por ejemplo, con las direcciones IP atribuidas a un ordenador instalado en un cibercafé, en el que no se pide identificación alguna a los clientes. En este caso, puede argüirse que los datos recogidos sobre el uso de un determinado ordenador "X" durante una determinada franja horaria no permiten la identificación del usuario con medios razonables y, por lo tanto, no son datos personales. Sin embargo cabe señalar que, muy probablemente, los prestatarios de servicios de Internet no sabrán si la dirección IP en cuestión permite la identificación o no, y tratarán los datos asociados a esa IP de la misma manera que tratarían la información asociada a las direcciones IP de los usuarios debidamente registrados e identificables. Así pues, a menos que el prestatario de servicios de Internet sepa con absoluta certeza que los datos corresponden a usuarios que no pueden ser

identificados, tendrá que tratar toda información IP como datos personales, para guardarse las espaldas.

4.- "Persona física" como concepto al que se refiere el artículo 6 de la Declaración Universal de los Derechos Humanos, así "*todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica.*". El considerando 2 de la Directiva así lo establece explícitamente al afirmar que "*los sistemas de protección de datos están al servicio del hombre*" y que "*deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales*". Los datos personales son, por lo tanto, datos relativos a *seres vivos* identificados o identificables *a priori*.

En principio, la información relativa a personas fallecidas no se debe considerar como datos personales sujetos a las normas de la Directiva, ya que los difuntos dejan de ser personas físicas para el Derecho Civil. Sin embargo, en determinados casos los datos de los difuntos, incluso pueden recibir indirectamente una cierta protección.

En cuanto al *nasciturus*, la medida en que las normas de protección de datos pueden aplicarse antes del nacimiento de una persona depende de la posición general de los ordenamientos

jurídicos nacionales respecto a la protección del concebido pero no nacido.

Dejando ya fijado el concepto de "datos personales", y volviendo a la regulación comunitaria respecto de su tratamiento[247], más concretamente respecto del tratamiento total o parcialmente automatizado de datos personales, así como el no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, se impone que sean:

a) Tratados de manera leal y lícita.

b) Recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas.

c) Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.

[247] Entendido como *"cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción",* de conformidad con el artículo 2,b) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

d) Exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados.

e) Conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

Este tratamiento de datos personales sólo puede efectuarse si:

a) El interesado ha dado su consentimiento de forma inequívoca, o…

b) Es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o…

c) Es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o…

d) Es necesario para proteger el interés vital del interesado, o…

e) Es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o…

f) Es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

En caso de obtención de datos recabados del propio interesado, el responsable del tratamiento o su representante deberán comunicar a la persona, de quien se recaben los datos, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:

a) La identidad del responsable del tratamiento y, en su caso, de su representante.

b) Los fines del tratamiento de que van a ser objeto los datos.

c) Cualquier otra información, tal como:

- Los destinatarios o las categorías de destinatarios de los datos.
- El carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder.
- La existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, como regla general, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello:

a) La identidad del responsable del tratamiento y, en su caso, de su representante;

b) Los fines del tratamiento de que van a ser objeto los datos;

c) Cualquier otra información tal como:

- Las categorías de los datos de que se trate.
- Los destinatarios o las categorías de destinatarios de los datos.
- La existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

Se impone al responsable del tratamiento la obligación de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados (en particular, cuando el tratamiento incluya la transmisión de datos dentro de una red), y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel

de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

No hay duda de que los datos relativos al lugar de ubicación de un objeto y al trazado de sus eventuales desplazamientos, siempre que se vincule o pueda ser vinculado a una persona física sirviendo a la identificación de ésta, integra el concepto de dato de carácter personal[248]. Para que un dato de carácter personal quede sujeto al régimen de tutela de la LOPDCP y su Reglamento es necesario que la actuación respecto de tales datos corresponda a una operación incluida en el concepto de "tratamiento"[249], entendiendo por tal, según su artículo 3.c) las *"operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*". Los datos de localización, que sufren un tratamiento de carácter automatizado (artículo 3.1. Directiva 95/46/CE), integran sin duda alguna, esta

[248] Así lo entiende en diversos informes, el Gabinete Jurídico de la Agencia Española de Protección de Datos (AEPD) donde son precisados diferentes aspectos de los datos que permiten la localización geográfica. El citado órgano se ha pronunciado mediante sucesivos informes, entre otras materias, en relación con los datos emitidos por GPS instalados en vehículos (Informe 193/2008), la geolocalización de los accesos a portales de juego *on-line* (Informe 216/2008), la traslación a personas jurídicas de las normas de protección de datos en relación con los de tráfico y localización en telecomunicaciones (Informe 420/2008), la lectura de matrículas por la policía en un aparcamiento público (Informe 433/2008) o el tratamiento de datos de localización de empleados en tarea de escolta mediante los datos GPS enviados por teléfonos móviles (Informe 640/2009).

[249] Para PÉREZ GIL, "tratamiento de datos" es una noción comprensiva de todas aquellas operaciones y procedimientos que permitan realizar al menos una de las actuaciones que mencionan los preceptos 3.c) de la LOPDCP. De ello se deriva que cualquiera de esas actuaciones (recoger, grabar, conservar, etc.) será, en sí misma, constitutiva de "tratamiento", como viene a plasmar el art. 5.1.c) RPDCP, al definir la "cesión o comunicación de datos" de la siguiente manera: "Tratamiento de datos que suponen su revelación a persona distinta del interesado".

Vid., PÉREZ GIL, J., *Los datos sobre localización geográfica…*, *op. cit.*

categoría, de ahí, que se considere su posible afección al derecho a la protección de datos personales consagrado en el artículo 18.4 de la Constitución Española[250].

En el ámbito nacional, se ha de aplicar la Ley 9/2014 de 9 Mayo, General de Telecomunicaciones, que regula en su artículo 41 la "Protección de los datos de carácter personal", y ello sin perjuicio de la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

Así los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal. Dichas medidas incluirán, como mínimo:

---

[250] Recordado por PÉREZ GIL, el Tribunal Constitucional define este derecho en su sentencia 292/2000, FJ 5, como "*un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".* La garantía opera sobre datos de muy diversa naturaleza, siempre que "*tangan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado"* sentencia del Tribunal Constitucional 292/2000, FJ 6.

Vid., PÉREZ GIL, J., "El nuevo papel de la telefonía móvil en el proceso penal…", *op. cit.*, p.150.

a) La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la Ley.

b) La protección de los datos personales almacenados o transmitidos, de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos.

c) La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.

En caso de que exista un riesgo particular de violación[251] de la seguridad de la red pública o del servicio de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

En caso de violación de los datos personales, el operador de servicios de comunicaciones electrónicas disponibles al público notificará sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos. Si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o

[251] Se entenderá como violación de los datos personales, la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo, en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público.

particular, el operador notificará también la violación al abonado o particular, sin dilaciones indebidas.

La notificación de una violación de los datos personales a un abonado o particular afectado no será necesaria, si el proveedor ha probado, a satisfacción de la Agencia Española de Protección de Datos, que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad. Unas medidas de protección de estas características podrían ser aquellas que convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos.

Principal es la LO 15/1999, de 13 Diciembre, de Protección de Datos de Carácter Personal (LOPDCP), la cual tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales[252], las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente de su honor e intimidad personal y familiar.

Esta normativa es de aplicación a los datos de carácter personal[253] registrados en soporte físico, que los haga susceptibles de tratamiento, y

[252] "Tratamiento de datos" como operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias, de conformidad con el artículo 3,c) LOPDCP.

[253] "Dato de carácter personal" entendido como cualquier información concerniente a personas físicas identificadas o identificables, de conformidad con el artículo 3,a) LOPDCP.

a toda modalidad de uso posterior de estos datos por los sectores público y privado, siempre que:

- El tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento, o…

- Al responsable del tratamiento no establecido en territorio español le sea de aplicación la legislación española, en aplicación de normas de Derecho Internacional Público, o…

- Al responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice, en el tratamiento de datos, medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

Quedan excluidos del ámbito de aplicación de esta norma:

- Los ficheros[254] mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

- Los ficheros sometidos a la normativa sobre protección de materias clasificadas.

[254] "Fichero" entendido como todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso, de conformidad con el artículo 3 b) LOPDCP.

- Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará, previamente, la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

Como regla general, el tratamiento de los datos de carácter personal requerirá el consentimiento[255] inequívoco del afectado, salvo que la ley disponga otra cosa. Excepcionalmente, no será preciso dicho consentimiento:

- Cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias.

- Cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.

- Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado (para la prevención o para el diagnóstico médicos, para la prestación de asistencia sanitaria o para tratamientos médicos o la gestión de servicios sanitarios, siempre

[255] "Consentimiento del interesado" como toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen, de conformidad con el artículo 3 h) LOPDCP.

que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto, o para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento).

- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

El consentimiento podrá ser revocado por causa justificada.

Los datos de carácter personal, objeto del tratamiento, sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. Si bien, este consentimiento no es preciso cuando la comunicación que deba efectuarse tenga por destinatario, entre otros, al Ministerio Fiscal o los a Jueces o Tribunales, en el ejercicio de las funciones que tiene atribuidas (tal es el caso de los datos de geolocalización interesantes para la instrucción de una causa).

Así las cosas, y dejando a un lado lo anterior, la habilitación legal para la incautación policial del dispositivo GPS o del terminal electrónico que lo contenga está permitida por los artículos 334 y 574 LECrim. y a los cuerpos policiales les es exigida por los artículos 282 y 770.3 LECrim., y en lo que pudiera incidir en datos que afectaran el derecho a la protección del dato personal automatizado (artículo 18.4 CE), tendría la cobertura del artículo 22 LOPD[256].

La LO 13/2015, de 5 de octubre deja claro en la nueva redacción que otorga a la Ley de Enjuiciamiento Criminal que, los datos obrantes en archivos automatizados de los prestadores de servicios (artículo 588 ter j) solo podrán ser cedidos para su incorporación al proceso con autorización judicial, debiendo ser estos solicitados, cuando el conocimiento de los mismos sea indispensable para la investigación, al Juez competente a los efectos de lograr autorización.

III.- GEOLOCALIZACIÓN A TRAVES DE DIRECCIONES IP

Debemos de partir de la posición de la jurisprudencia en relación a la dirección IP, la cual afirma que, aunque sí identifica a un ordenador determinado con una concreta conexión, no lo hace por sí respecto del usuario, por lo que no se precisa autorización judicial para conseguir lo

[256] VELASCO NÚÑEZ, E., *Tecnovigilancia, geolocalización y datos…*, *op. cit.*

que es público y no se encuentra protegido ni por el apartado 1 ni por el 3 del artículo 18 de la Constitución Española[257].

La obtención de esa IP, en el sentido de conexión a Internet, no ha de considerarse como comunicación, y sí como presupuesto técnico necesario para hacerla posible[258].

Cuestión distinta de la conexión técnica como tal, son las subsiguientes actuaciones de identificación y localización de la persona que tiene asignado esa IP, ya que éstas sí se deben efectuar al amparo judicial, pues a diferencia de la dirección IP, el nombre del usuario al que corresponde es un dato proporcionado al proveedor en el marco de una relación contractual sometido únicamente al régimen de protección de datos. Así, la averiguación de la dirección IP estática ha de considerarse como dato de suscripción, mientras que si fuera dinámica se hallaría vinculada a una comunicación concreta.

Lo anterior se complica aún más cuando se utiliza para la navegación, una dirección IP de un servidor que no aporta datos sobre sus usuarios, de modo que se logra poner un intermediario entre el

[257] Sentencias del Tribunal Supremo, Sala Segunda, 292/2008, de 28 de mayo, y 776/2008, de 18 de noviembre.

[258] GONZÁLEZ LÓPEZ sostiene que *"entender que la conexión a Internet, que no necesariamente debe ir acompañada de una comunicación concurrente, constituye una comunicación es equiparable a sostener la condición de comunicación del envío de la señal a la antena de telefonía móvil a efectos de la ubicación del terminal en una área de cobertura. A nuestro entender, estas actuaciones técnicas, si bien pueden considerarse comunicación desde un punto de vista técnico, escapan al propósito ya apuntado de la comunicación (envío de mensaje emisor a receptor) y constituyen, por ello, un presupuesto técnico necesario para hacer posible la comunicación"*

Vid., GONZÁLEZ LÓPEZ, J. J., *Intervención de las comunicaciones…*, *op. cit.*, p. 86.

ordenador y la web o el servicio al que se accede, quedando únicamente en éste solo los datos del servidor, pero no los del usuario. Estos intermediarios son conocidos como servidor *Proxy*[259].

En cualquier caso, y aunque no se hiciera uso de un Proxy, la dirección IP únicamente señalaría a un *router*, a través del cual pueden salir a Internet diversos ordenadores conectados al mismo tiempo, localizando el lugar desde el que se ha producido la conexión, pero, en ningún caso, el usuario y quizás tampoco, si existen varios, el equipo concreto. Solo existe una posibilidad al respecto de la identificación del terminal determinado en uso, y es analizando la dirección MAC o identificador de la tarjeta red de la que cada ordenador dispone para conectarse a un *router*, pudiendo a veces dicha dirección viajar en algunos paquetes de información que se usan para la navegación por Internet, dato que podría ser muy útil en el seno de una investigación[260].

---

[259] "*Estos intermediarios son conocidos como servidor Proxy y sus direcciones IP pueden ser fácilmente encontradas en Internet tecleando "Proxy Server list" en cualquier buscador. Esta búsqueda nos redirigirá a multitud de páginas web, muchas de las cuales se encuentran establecidas en países como Rusia […]. Muchos de estos Proxy son ordenadores que por estar mal configurados permiten el acceso a usuarios anónimos […] pero otros muchos son servidores estratégicamente situados en países a los que resulta sumamente difícil acceder como Vietnam o China y en los que raramente se van a guardar los logs sobre las conexiones realizadas.[…]".*

FERNÁNDEZ LÁZARO, F., *Medios técnicos en la investigación de los delitos informáticos*, en VELASCO NÚÑEZ, E. (Dtor.), "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia", Consejo General del Poder Judicial, Madrid, 2007.

[260] La dirección MAC es un identificador hexadecimal de 48 bits que se expresa por seis pares de números hexadecimales, asignado directamente por el fabricante de los dispositivos y que no puede ser repetido, aunque sí modificado a través de una operación compleja conocida como *MAC Spoofing* haciendo uso de programas específicos o bien mediante el propio sistema operativo.

III.1.-Rastreo policial de la IP

Útil es en este punto desarrollar la postura del Tribunal Supremo en relación con la captación de la dirección IP, por parte de unidades policiales especializadas en delitos tecnológicos, de accesos realizados por usuarios que se interconectaron con programas informáticos de intercambio de archivos con contenidos de pornografía infantil, a través de los cuales se obtenía información sobre las IP atribuidas a los usuarios.

Los usuarios así identificados intercambiaban gratuitamente sus archivos a través de programas P2P (*peer to peer*), que permiten el acceso a sus terminales informáticos, así como la transmisión o copia de programas, archivos o documentos allí almacenados. Estos programas, tales como EMULE o EDONKEY, comparten nodos que interactúan entre sí facilitando el intercambio de toda clase de archivos de audio, video, software…, optimizando el rendimiento en la transferencia por su actuación global, donde no existen realmente ni servidores ni usuarios. Su éxito radica en que cualquier usuario de terminal informático puede adentrarse directamente en el contenido de todos los terminales interconectados con solo entrar en las direcciones web de los respectivos dominios P2P[261].

[261] Conforme a la sentencia del Tribunal Supremo, Sala Segunda, 167/2016, de 2 de marzo, *"la aplicación emule es una plataforma gratuita una plataforma gratuita ideada para el intercambio de archivos entre usuarios conectados a través de la misma, siendo uno de los denominados programas P2P (peer to peer), de los que existen diversas variantes en internet para las distintas redes de intercambio, todas ellas con*

Es en esta dimensión abierta, del libre acceso consentido, donde la actuación policial ha tenido su encaje, plenamente lícito, a través de técnicas de rastreo de los accesos a los *hash* que contenían imágenes de pornografía infantil, y de los que se podía extraer, porque así lo publicaban junto con la imagen, los accesos que se habían producido a las mismas. Se trata de una información accesible a cualquier persona, un rastro dejado por los usuarios que accedían a tales contenidos, en condiciones tales que podía ser seguido por cualquier persona sin traba ni limitación alguna; pero a través de tal fuente solamente se puede acceder al dato impersonal, numérico, de determinada IP y de la hora y fecha del acceso, requiriéndose para el siguiente paso, para el conocimiento de la persona que está detrás de tal acceso, de la previa autorización judicial para el recabo de tal información.

Así, en este entorno, se dicta la sentencia del Tribunal Supremo, Sala Segunda, 1058/2006, de 2 de noviembre, referida al empleo, no de redes P2P, sino de chats abiertos, accediendo a la información mediante el rastreo de las *file servers*. Un defecto de fondo en el contenido del recurso impidió al tribunal pronunciarse sobre la licitud del acceso a los

funcionamiento semejante no existiendo un servidor central en el que se almacenan los contenidos y al que se pueda acceder para evitar su difusión, tratándose de una aplicación que no tiene clientes ni servidores fijos, y si uno de los usuarios inicia la descarga de un archivo, instantáneamente se convierte en servidor de la parte del archivo que ha descargado, posibilitando a un tercero iniciar la descarga simultanea desde su propia carpeta compartida del archivo incompleto recibido. Por tanto, y a grandes rasgos, la red emule es la unión de todos los usuarios de la misma, y los servidores, que son clientes con características especiales, permiten mantener a todos los clientes conectados unos con otros; y todo aquel que se instala un programa cliente de redes P2P forzosamente tiene que conocer que se trata de una red de usuarios que comparten parte de los contenidos de sus ordenadores.".

números IP utilizados. Mismo problema hubo con la sentencia del Tribunal Supremo, Sala Segunda, 921/2007, de 6 de noviembre.

Continuando con la temática del rastreo policial de la IP, la sentencia del Tribunal Supremo 236/2008, de 9 de mayo[262], se planteó *"la duda, de si para solicitar el número telefónico o identidad de una terminal telefónica (cabría extenderlo a una dirección o identificación de Internet: Internet Protocols), es necesario acudir a la autorización judicial, si no han sido positivas las actuaciones policiales legítimas integradas por injerencias leves y proporcionadas, que puede respaldar la Ley Orgánica de Cuerpos y Fuerzas de Seguridad del Estado o Ley de Seguridad Ciudadana, en la misión de los agentes de descubrir delitos y perseguir a los delincuentes"*, concluyendo que los datos identificativos de un titular o de una terminal deberían ser encuadrados, no dentro del derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución Española), sino en el marco del derecho a la intimidad personal (artículo 18.1 de la Constitución Española) con las excepciones legales, en relación a la necesidad de autorización judicial para recabar según qué datos[263].

[262] Esta línea ha sido seguida por sentencias del Tribunal Supremo, Sala Segunda, tales como 292/2008, de 28 de mayo, y 680/2010, de 14 de julio.

[263] LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal o su Reglamento, Real Decreto 1720/2007 de 21 de diciembre, que entró en vigor el 31 de marzo de 2008, sin despreciar la extinta Ley 32 de 3 de noviembre de 2003, General de Telecomunicaciones y su Reglamento, RD 424/2005 de 15 de abril de 2005, normativa que fue sustituida por la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, así como Ley 25/2007, de 18 de octubre de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación, dictada en desarrollo de la Directiva de la Unión Europea 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo.

Aún es mas, quien utiliza un programa P2P asume que muchos de los datos se convierten en públicos para los usuarios de Internet, circunstancia que conocen o deben conocer los internautas, siendo asimismo dichos datos conocidos por la policía, datos públicos en Internet, los cuales no se hallan protegidos por el artículo 18.1 ni por el 18.3 de la Constitución Española.

Así, la autorización, en opinión del Alto Tribunal, quedaría reservada para desvelar la identidad de la persona que está detrás de la utilización de determinada dirección IP, relacionada con un concreto acceso público. Continua con el mismo tenor, entre otras, la sentencia del Tribunal Supremo, Sala Segunda, 292/2008, de 28 de mayo[264], poniendo de manifiesto, de manera destacable, que *"La complejidad de la materia, su ductilidad, y las singulares características de la normativa que la regula, hace necesario que futuras resoluciones de esta Sala vayan*

[264] Sentencia del Tribunal Supremo, Sala Segunda, 292/2008, de 28 de mayo, FJ9: *"cuando la comunicación a través de la Red se establece mediante un programa P2P, como en el EMULE o EDONKEY, al que puede acceder cualquier usuario de aquélla, el operador asume que muchos de los datos que incorpora a la red pasen a ser de público conocimiento para cualquier usuario de Internet, como, por ejemplo el IP, es decir, la huella de la entrada al programa, que queda registrada siempre. Y fue este dato, el IP del acusado, el que obtuvo la Guardia Civil en su rastreo de programas de contenido pedófilo, dato que -conviene repetir y subrayar- era público al haberlo introducido en la Red el propio usuario -el acusado- al utilizar el programa P2P. Por ello, no se precisa autorización judicial para conocer lo que es público, y esos datos legítimamente obtenidos por la Guardia Civil en cumplimiento de su obligación de persecución del delito y detención de los delincuentes, no se encuentran protegidos por el artículo 18.3 de la Constitución Española. Porque, debe recordarse, el IP del acusado que averiguó la Guardia Civil, no identifica la persona del usuario, lo que hace necesario para conocer el número del teléfono y titular del contrato la autorización judicial, que es lo que se hizo aquí, pues la Policía judicial a través de un oficio de 6 de noviembre de 2005, completado por un informe de 24 de octubre del mismo año del Grupo de delitos telemáticos de la Guardia Civil interesa la preceptiva autorización que obtuvo con el libramiento de mandamiento judicial dirigido a los operadores de Internet para identificar ciertas direcciones IP del ordenador al objeto de proseguir la investigación".*

perfilando un cuerpo de doctrina atendiendo a las peculiaridades de cada caso en concreto".

Otras resoluciones del Alto Tribunal a este respecto, que mantiene inalterada su postura de defender la licitud del rastreo policial de IP a través de lugares accesibles a cualquiera (redes P2P) en su labor de investigación criminal, son las Sentencias del Tribunal Supremo, Sala Segunda, 680/2010, de 14 de julio o la 247/2010, de 18 de marzo.

Mención concreta merece la sentencia del Tribunal Supremo, Sala Segunda, 680/2010, de 14 de julio, ya que entra de lleno en la cuestión de la compatibilidad de la línea jurisprudencial anteriormente expuesta con las bases de datos relativos a las comunicaciones creados al amparo de la Ley 25/07 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación, y sienta la premisa de que tales bases de datos no excluyen la posibilidad de obtener la misma información por canales lícitos diversos, entre los que se encuentran, sin duda, aquellas fuentes que los propios usuarios hacen permeables, sin restricción alguna, al acceso a cualquier persona.

III.2.- Cesión de datos por los sujetos obligados

Como consecuencia de la transposición de la Directiva 2006/24/CE[265], surge la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Tras la entrada en vigor de esta Ley, se hace necesario el mandato judicial para oficiar a la operadora y que ésta proporcione la información relativa a una determinada IP[266], y ello a pesar de que el dato no pueda cobijarse bajo el manto protector del secreto de las comunicaciones.

Pese a las objeciones de la Fiscalía, que veía limitada con ello su capacidad de acción dentro de su función de promover la justicia, dado que sus peticiones de información a los ISP serían denegadas, el Tribunal Supremo adoptó, en línea continuista con la norma, el Acuerdo no Jurisdiccional de 23 de febrero de 2010, en relación con esta necesidad

[265] El artículo 1 de la Directiva 2006/24/CE fija como objeto de la misma armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro, siendo aplicable a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado.

Esta Directiva 2006/24/CE ha sido anulada por la STJUE, Gran Sala, de 8 de abril de 2014 debido a la escasa definición en la norma de las cautelas y garantías jurídicas precisas y claras que exige la inmisión en el derecho a la protección de datos personales.

[266] Antes de la aprobación de la Ley 25/2007, el artículo 12 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE), fijaba el marco jurídico para el tratamiento y la cesión de los datos, entre los que se hallaba la IP (derogado actualmente). Así, en su artículo 12, se establecía que estos datos quedaban a disposición de Jueces y Fiscales en el marco de investigaciones criminales o para la salvaguardia de la seguridad pública y la defensa nacional. Para el caso de las Fuerzas y Cuerpos de Seguridad del Estado, esta cesión se debía de realizar de conformidad con la normativa de protección de datos de carácter personal.

de autorización judicial para la cesión de datos de las operadoras de comunicaciones, supliendo la laguna legal afirmando lo siguiente:

"Es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Ministerio fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007, de 18 de octubre".

Sin perjuicio de que ha quedado clara la necesidad de actuación judicial, no lo es tanto la naturaleza de los datos que se recaban de los sujetos obligados. Así por ejemplo, para GONZÁLEZ LÓPEZ[267] si la obtención de la dirección IP se efectúa en el marco de una intervención de las comunicaciones, el conocimiento de los "datos de conexión" se vincula a comunicaciones determinadas y, debido a ello, se erigen como información comprendida en el secreto de las comunicaciones.

Por su parte, la sentencia del Tribunal Supremo, Sala Segunda, 247/2010, de 18 de marzo[268], que interpreta la doctrina existente, distingue entre los datos personales que pueden afectar al secreto a las comunicaciones, y cuándo los conservados y tratados por las operadoras, no se están refiriendo a comunicación alguna, es decir, datos

[267] GONZÁLEZ LÓPEZ, J. J., "Intervención de las comunicaciones…", *op. cit.*, p. 86.

[268] Que dice reconocerse heredera de las sentencias del Tribunal Supremo, Sala Segunda, 236/2008, de 8 de mayo, y 292/2008, de 28 de mayo, así como de la doctrina sentada en la sentencia del caso Malone.

estáticamente almacenados, conservados y tratados por operadores que se hallan obligados a la reserva frente a terceros. Así, distingue dos conceptos:

a) Datos personales externos o de tráfico, que hacen referencia a una comunicación concreta y contribuyen a desvelar todo o parte del secreto que protege el artículo 18.3 de la Constitución Española.
b) Datos o circunstancias personales referentes a la intimidad de una persona (artículo 18.1 de la Constitución Española), pero autónomos o desconectados de cualquier comunicación, que caerán dentro del derecho a la protección de datos informáticos o *habeas data* del artículo 18.4 de la Constitución Española que no pueden comprometer un proceso de comunicación.

Aunque pudiera parecernos en una primera lectura que la sentencia está distinguiendo lo que podría definirse como la dimensión estática frente a la dinámica del dato relativo a las comunicaciones, lo cierto es que lo que hace realmente es romper con el principio de la protección formal del secreto de las comunicaciones, al establecer un auténtico criterio de exclusión de aquellos que se definen como datos personales externos o de tráfico (primera esfera de protección), cuya menor incidencia en el secreto de las comunicaciones haría más

adecuado residenciarlos en el ámbito de la protección de simples datos de carácter personal[269].

En este caso concreto, el Ministerio Fiscal, y no la policía, solicita la identidad del titular de un terminal informático, entendiendo la sentencia que *los datos cuya obtención se pretende por el Fiscal no tienen relación ni afectan ni interceptan ni descubren ni tratan de descubrir una comunicación concreta, sino que por ser preciso para la acción investigadora el conocimiento del domicilio, número de teléfono o identidad del titular del terminal informático que opera en la Red (IP), la solicita a la operadora, al objeto de pedir del juez un mandamiento de entrada y registro con fines indagatorios o de investigación de un posible delito, acerca del que se conocen datos indiciarios.* Tal proceder del Ministerio Fiscal no afecta al secreto de las comunicaciones, sino que se desenvuelve en el marco del derecho a la intimidad, más concretamente dada la escasa intensidad en que es efectuada, la cuestión se proyectaría sobre la obligación que establece la Ley Orgánica de Protección de Datos de no publicar los datos personales de los usuarios que un servidor de Internet posee, los cuales no pueden cederse sin el consentimiento del

[269] Opinión compartida por DÍAZ CAPPA. Expone el autor que *"la absoluta equiparación de todo tipo de datos de tráfico o la inclusión de todo ellos dentro del derecho al secreto de las comunicaciones, comportaría un auténtico desenfoque del problema".*

DÍAZ CAPPA, J., *Confidencialidad, secreto de las comunicaciones e intimidad en el ámbito de los delitos informáticos*, Diario La Ley, núm. 7666, Sección Doctrina, Año XXXII, Ref. D-272, Editorial LA LEY, 5 julio 2011.

titular, pero la ley establece diversas excepciones, entre las que se encuentra este supuesto[270].

Sin duda alguna, los datos relativos a la IP, como la localización, que pueden ser recabados de los sujetos obligados no son datos de tráfico ni tampoco gozan de la protección que otorga el artículo 18.3 de la Constitución Española, puesto que no están inmersos dentro de comunicación alguna, ni asociados a ella. La ubicación de su regulación dentro de la Ley de Enjuiciamiento Criminal así lo avala al encontrarse dentro de la Sección 3ª del Capítulo V, Título VII del Libro II, y no de la Sección 2ª dedicada a la *Incorporación al proceso de datos electrónicos de tráfico o asociados.* En refuerzo de nuestra posición, VELASCO[271], entre otros juristas, niega que sea un dato de tráfico la ubicación de la dirección IP como "datos contractuales asociados", y entiende que

[270] El artículo 11.2 d) de la Ley Orgánica 15/1999 de 13 de diciembre nos dice que el consentimiento del interesado a que se refiere el párrafo anterior no será necesario.... d) *"Cuando la comunicación que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales o el Tribunal de Cuentas en el ejercicio de las funciones que tienen atribuidas".*

Por su parte, la Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones (aplicable en el supuesto que tratamos, y derogada por la Ley 9/2014, de 9 de mayo), cuyo articulado se remitía al art. 12 de la Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (ahora derogada por la Ley 25/2007), establecía el deber de retención de datos de tráfico relativos a las comunicaciones electrónicas, más concretamente declaraba que los *"datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguarda de la seguridad pública y la defensa nacional, poniéndola a disposición de los jueces o tribunales o del Ministerio Fiscal que así lo requieran"* .

Actualmente, la vigente la Ley 9/2014, de 9 de mayo, determina en su artículo 42 que *la conservación y cesión de los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.*

[271] VELASCO NÚÑEZ, E., "Delitos cometidos a través de Internet. Cuestiones procesales", 1ª edición, Editorial LA LEY, Madrid, junio 2010, p.149.

continúan rigiéndose por la LOPD, ya que no son datos técnicos sino contractuales referentes a comunicaciones[272].

Otro problema añadido que se ha planteado ha sido que conforme al objeto de la Ley 25/2007, de 18 de octubre, únicamente podrá autorizarse judicialmente la cesión de datos para aquellas investigaciones dedicadas a delitos graves. Así, si nos fijamos, la gran mayoría de los delitos cometidos a través de Internet, se encuentran castigados con una pena de prisión menor a los cinco años[273], de modo que tanto los Juzgados de Instrucción como los investigadores se encuentran atados de pies y manos en estos supuestos. Resulta en cualquier caso paradójico que se admita la adopción de la prisión provisional, según el artículo 503.1 de la Ley de Enjuiciamiento Criminal, para delitos con penas iguales o superiores a dos años, o incluso menos, en otros supuestos, y sin embargo, se requiera que el delito que se pretenda investigar a través

[272] Frente a ello, se erige MAEZTU que entiende que dicha línea de pensamiento dejaría sin contenido no solo a la LCD, sino a la Directiva 2006/24/CE. Partiendo de la propia *ratio legis*, afirma que los datos que identifican a un usuario en relación a una IP, con independencia de que deban o puedan servir al ISP para prestar el servicio y para su facturación, es un tipo de datos sujeto a la LCD. El artículo 3 de la LCD expresamente dispone que: "*1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes: […] a) Datos necesarios para rastrear e identificar el origen de una comunicación: […] 2º Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet: […] iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono*".

Vid., MAEZTU LACALLE, D., *La identificación del titular de una dirección IP. Problemática en aplicación de la Ley 25/2007, de conservación de datos*, en PÉREZ GIL, J. (Dtor.) "El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito", Editorial LA LEY, Madrid, 2012, p. 213.

[273] Conforme al Código Penal, por ejemplo las amenazas (artículo 169, únicamente las condicionales en su grado máximo alcanzarían los cinco años), difusión, venta o exhibición de material pornográfico entre menores de edad o incapaces (artículo 186), calumnias (artículo 206), injurias (artículo 209), o el delito de estafa (tipo básico, artículo 249).

de la cesión de datos sobre la IP esté castigado con pena mínima de cinco años de prisión.

En contestación a estas dudas, MAEZTU[274] recuerda varias argumentaciones jurídicas para superar o reinterpretar esa limitación legal, buscando una redefinición del concepto de delito grave para poder así ampliar las posibilidades de investigación y de obtención de la identificación del usuario de la dirección IP en aquellos supuestos de delitos con pena menor a cinco años:

- La referencia a los delitos graves no es literal, puesto que esta clasificación de los delitos es extraño al resto de los ordenamientos jurídicos europeos. Visto así, la Directiva ha de observarse bajo este condicionante que justifica la ampliación a delitos castigados con pena de menos de 5 años, puesto que, de otro modo, la transposición de la misma ha sido errónea.

- Que el criterio usado por el del Código Penal para la clasificación de los delitos es meramente formal, y no material, y tiene como única finalidad ordenar procesalmente la atribución de competencias a las Audiencias Provinciales.

[274] MAEZTU LACALLE, D., *La identificación del titular de una dirección IP…*, *op. cit.*, p. 215.

- Que esta limitación a la investigación es una quiebra de la tutela judicial efectiva del artículo 24 de la Constitución Española, debiéndose tener en cuenta sentencias del Tribunal Constitucional, como la 104/2006, sobre la superación del concepto formal de los delitos graves.

En conclusión, los rastreos policiales para localizar direcciones IP podrían, por tanto, realizarse sin necesidad de autorización judicial, ya que no se trata de datos confidenciales preservados del conocimiento público cuando estamos ante un dato que el propio interesado ha permitido sea de público conocimiento[275], sin perjuicio de que se informe al Juez de Instrucción competente, si derivado de ello se solicita

[275] Sentencia del Tribunal Supremo, Sala Segunda, 292/2008, de 28 de mayo, FJ10: "*No cabe negar que la Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, da un paso de gigante -excesivo o desmesurado según la doctrina científica especializada-, al desarrollar la Directiva de la Unión Europea 2006-24 C.E. del Parlamento Europeo y del Consejo. Esta Ley tiene por objeto imponer la obligación a los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos con el fin de entregarlos a los agentes facultados, en caso de que le fueran requeridos por éstos, entendiendo por tales agentes los pertenecientes a los Cuerpos Policiales, al Centro Nacional de Inteligencia y a la Dirección de Vigilancia Aduanera. Esta Ley exige para la cesión de estos datos, con carácter general, la autorización judicial previa y entre los datos que deben conservar figura el que es objeto del proceso que nos ocupa, es decir "la identificación del usuario asignada" en el acceso a Internet, como expresamente establece el art. 3.a.2º.i), así como "el nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de protocolo de Internet (IP), una identificación de usuario o un número de teléfono". Por su parte, el art. 7 (procedimiento de cesión de datos) determina que los datos a los que se refiere el art. 3 necesitarán una resolución judicial para su cesión a los funcionarios policiales, con lo que, en principio, parece claro que la obtención del IP se encuentra sometida a esta exigencia, lo cual no resulta muy congruente con el hecho tantas veces repetido en esta resolución de que la obtención de ese dato por los servicios policiales se produjo lícitamente, con lo cual la incongruencia se convierte en absurdo cuando se requiere por la norma una autorización judicial para acceder a un dato que el propio interesado ha permitido ser de público conocimiento. Cuestión distinta será en los supuestos en los que en las diligencias de investigación desarrolladas por las Fuerzas y Cuerpos Policiales en la persecución de actividades delictivas de cualquier naturaleza para cuyo progreso sea necesario conocer el IP (o el número telefónico) de una determinada persona que hasta el momento es desconocido, se tenga que acatar esa exigencia legal".*

autorización judicial para intervención de las comunicaciones o registro de dispositivo. Otra cosa distinta sería que no se vaya a realizar rastreo alguno y se solicite a la autoridad judicial, por parte de los investigadores, en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en Internet, la identificación y localización del equipo o del dispositivo de conectividad correspondiente o los datos de identificación personal del usuario, para su requerimiento a los sujetos obligados por el deber de colaboración, debiéndose entonces cumplir lo dispuesto el artículo 588 ter k de la ley de Enjuiciamiento Criminal.

En el momento presente, estando clara la necesidad de autorización judicial y que el delito investigado sea de los castigados con pena grave, como así expresamente se dispone en el articulado de la Ley, queda fuera todo tipo de interpretación extensiva, ya que la norma es clara al respecto. Dicho lo cual, ello no es óbice para que sea imprescindible reducir ese tope penológico que limita los delitos a investigar, dado que en la práctica se hace harto complicado la concesión de una autorización judicial para la investigación del titular de una IP siempre que se quiera ser riguroso con la norma.

IV.- ETIQUETAS INTELIGENTES CON TECNOLOGÍA WIFI

La cada vez más generalizada interacción de dispositivos electrónicos automáticos que interactúan entre sí a través de diálogos que circulan por Internet (diálogos entre estaciones BTS y terminales de

telefonía móvil, etiquetas RDFI, actualización automática de programas informáticos o estados de redes sociales,…) plantea serios problemas a la hora de analizar su verdadera naturaleza jurídica y, sobre todo, si las mismas, pueden ser o no consideradas comunicaciones merecedoras de la protección formal del artículo 18.3 de la Constitución Española.

IV.1.- Diálogos automáticos entre dispositivos electrónicos que transitan a través de las redes de comunicaciones electrónicas

IV.1.A.- Conexiones e intercambio de información automática a través de Internet

Cuando ponemos en funcionamiento nuestro ordenador, sin necesidad de conectarlo a ningún navegador, entramos en contacto, transmitimos, y/o actualizamos información, como nuestra localización con determinados proveedores de software[276] o con otros servicios, tales

[276] *"Los sistemas operativos de ordenadores que trabajan con el entorno Windows están programados para que durante su encendido se conecten a los servidores de Microsoft. Éstos comprueban si hay actualizaciones o parches; y de haberlos, se procede a su descarga. Casi todas las aplicaciones utilizan el mismo sistema que Microsoft para chequear y actualizar las diferentes versiones de sus programas. En el caso de Microsoft, a partir del Windows 98 se creó un módulo llamado Windows Update, que a través de Internet contactaba con los servidores de Microsoft utilizando un ActiveX que permitía ver la información del sistema y descargar automáticamente las actualizaciones adecuadas. A partir de la versión XP, el sistema evolucionó hacia el actual Automatic Update, que se ha extendido al paquete Office y a otros programas gratuitos como el Windows Defender Anti-Spyware".*

como programas de detección de virus, así como permitimos la notificación de estados en redes sociales (avisos de disponibilidad y detección de usuarios activados, como sucede, por ejemplo con Skype); además compartimos archivos a través de programas P2P, actualizamos o accedemos a información a determinados canales de utilidades que se facilitan en la red, bajo las denominaciones técnicas de *gadgets* y *widgets*.

¿Dónde queda nuestra voluntad como usuarios respecto de todo lo anteriormente expuesto y de nuestra integración en las comunidades electrónicas? La intervención de la persona como beneficiario de estas redes no va más allá de la prestación de un consentimiento, a veces presunto, que no es más que la aceptación (en ocasiones porque no queda más remedio) de las condiciones de funcionamiento de cada red o la asunción de determinadas configuraciones, por defecto.

Si entendemos que interconexión (entendida como intercambio o acción de compartir información transmitida a través de la red de comunicaciones electrónicas) es sinónimo de comunicación, y defendemos que las comunicaciones electrónicas se encuentran amparadas por el secreto de las comunicaciones, cualquier examen judicial o policial, aunque fuera externo, como manifiesta RODRÍGUEZ LAÍNZ, de un PC abarcaría necesariamente contenidos de comunicaciones electrónicas, lo que daría protección al terminal bajo el

Vid., RODRÍGUEZ LAÍNZ, J. L., *Internet de los objetos…*, *op. cit.*

amparo del artículo 18.3 de la Constitución Española. De hecho, ejecutaríamos programas que, con toda seguridad, habrían sido descargados y actualizados a través de la red, adentrándonos en contenidos protegidos aparentemente por dicha norma constitucional. Por eso, para algunos autores[277], la solución que nos ofrece la Sentencia del Tribunal Constitucional 173/2011, de 7 de noviembre (que se tratara posteriormente), al escrutinio policial de ficheros *incoming* para comprobar el acceso a ficheros con contenidos pedófilos como origen de material de pornografía infantil descubiertos en un ordenador portátil, debería ser cuando menos sometida a una profunda reflexión.

IV.1.B.- Control y filtrado automático de comunicaciones electrónicas: el principio de neutralidad en la red

Con carácter previo a entrar en la materia, se hace preciso plasmar unas cuantas nociones básicas sobre transmisión de información a través de Internet, para un mejor entendimiento de la misma.

[277] RODRÍGUEZ LAÍNZ, J. L., *Hacia un nuevo entendimiento de la protección integral de los dispositivos privados de almacenamiento electrónico de datos relativos a las comunicaciones (Comentario a la STC 173/2011, de 7 de noviembre)*, Revista del Ilustre Colegio de Abogados de Madrid, Otrosí, 5ª Época, núm. 9, ICAM, enero-marzo de 2012.

En la misma línea crítica, ALCÁCER GUIRAO, R., *Derecho a la intimidad, investigación policial y acceso a un ordenador personal (Comentario a la STC 173/2011, de 7 de noviembre)*, La Ley Penal, núm. 92, Sección Jurisprudencia del Tribunal Constitucional, Editorial LA LEY, abril 2012.

Toda información que transmitimos por Internet se divide en paquetes, pudiendo los proveedores de servicios de Internet incluir en ellos, aparte de la información sobre el origen y el destino, otras capas y protocolos que se usaran para gestionar los distintos flujos de tráfico en la red[278].

Cada paquete tiene dos partes, la carga útil IP (*IP load*) que incluye el contenido de la información que va dirigida exclusivamente a su destinatario, y la cabecera de IP (*IP header*) que incluye, entre otros, la dirección del destinatario y del remitente. La cabecera de IP permite a los proveedores de servicios de Internet y a otros intermediarios encaminar la carga útil desde la dirección de origen a la dirección de destino. Los proveedores de servicios de Internet y otros intermediarios garantizan que los paquetes IP viajan a través de la red mediante nodos que leen la información de la cabecera de IP, lo comparan con las tablas de encaminamiento y luego las envían hacia el siguiente nodo, de camino a su destino. Este proceso se lleva a cabo a través de la red utilizando un enfoque "mejor esfuerzo sin memoria", ya que todos los paquetes que llegan a un nodo son tratados de una forma neutral. Cuando se envían al

[278] El Dictamen del Supervisor Europeo de Protección de Datos sobre la neutralidad de la red, la gestión del tráfico y la protección de la intimidad y los datos personales (DOUE 2012/C34/01) usa la analogía con la carta postal, de modo que entiende que utilizar un protocolo de trasmisión de red es equivalente a incluir el contenido de la carta en un sobre con una dirección de destino que pueda ser leída por el servicio postal y que éste pueda luego entregar. El servicio postal podrá utilizar protocolos adicionales en sus trámites internos para gestionar todos los sobres que deben transmitirse, siendo el objetivo que cada sobre llegue a su destino, tal como el remitente indicó en el origen.

siguiente nodo, no hay necesidad de conservar más información en el encaminador[279].

Ya en cuanto al principio de neutralidad en la red, este aparece regulado en el Dictamen del Supervisor Europeo de Protección de Datos sobre la neutralidad de la red, la gestión del tráfico y la protección de la intimidad y los datos personales (DOUE 2012/C 34/01), y hace referencia al debate en curso sobre si debe permitirse a los proveedores de servicios de Internet –PSI-[280] que limiten, filtre o bloqueen el acceso a Internet o que puedan afectar de otro modo su funcionamiento. Este concepto de neutralidad de la red se basa en la idea de que la información en Internet debe ser transmitida con imparcialidad, sin tener en cuenta el contenido, el destino o el origen, y que los usuarios deberían poder decidir qué aplicaciones, servicios y hardware desean utilizar.

No hay que olvidar que el filtrado, bloqueo y la inspección del tráfico de la red plantea cuestiones importantes en relación con el derecho al secreto de las comunicaciones y el respeto al derecho a la intimidad de las personas y de sus datos personales cuando utilizan

[279] Sin embargo, el equipo de red de Internet utiliza protocolos de encaminamiento que registran la actividad, procesan estadísticas de tráfico e intercambian información con otros equipos de red, a fin de encaminar los paquetes IP utilizando la vía más eficiente. Por ejemplo, cuando un enlace esta congestionado o roto y el encaminador recibe esta información, actualizara su tabla de encaminamiento con alguna alternativa que no utilice dicho enlace. Cabe asimismo señalar que la obtención y el tratamiento en algunos casos podrá hacerse con fines de facturación o incluso de conformidad con los requisitos de la Directiva de conservación de datos.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, Dictamen del Supervisor Europeo de Protección de Datos sobre la neutralidad de la red, la gestión del tráfico y la protección de la intimidad y los datos personales, DOUE 2012/C 34/01, nota (20).

[280] Se incluye el suministro tanto de acceso fijo como móvil a Internet.

Internet. Por ejemplo, determinadas técnicas de inspección implican la vigilancia del contenido de las comunicaciones, los sitios web visitados, los correos electrónicos enviados y recibidos, el momento en que esto tiene lugar y dónde etc., permitiendo el filtrado de comunicaciones.

Por tanto, podemos afirmar que el principio de neutralidad en la red nace como reacción a la tendencia de prestadores de servicios de Internet (PSI) a realizar discriminaciones, bloqueos y filtrados de comunicaciones en función de varios criterios ("políticas de gestión del tráfico"), entre los que se encuentran la cualidad del cliente a efectos comerciales o la política comercial de dar preferencia a determinados contenidos frente a otros (transferencia de datos frente a P2P,…). Por ello, tal principio orientador de la política de la Unión Europea pretende avanzar hacia el establecimiento de instrumentos jurídicos eficaces que instauren, a nivel normativo, la regla general de que tales operadores no puedan, a su elección, y salvo justificación técnica, dar prioridad o ralentizar el acceso a determinadas aplicaciones o servicios.

Visto lo anterior, como dice RODRÍGUEZ LAÍNZ, no se puede negar que un consentimiento explícito a tales sistemas de introspección técnica de carácter automático en contenidos de comunicaciones, por parte de PSI, podría sin duda ser considerado lícito; al menos en aquellos supuestos en que la política de la compañía respetara principios tan esenciales como, los de la no conservación de datos más allá de las necesidades de la prestación del servicio y de minimización o

proporcionalidad en su tratamiento. Sin embargo, evidentemente, cuando esta labor de inspección se escapa de las necesidades técnicas para llegar al nivel del control, filtrado e inspección indiscriminada de contenidos, el ámbito de lo lícito queda seriamente comprometido, ante la grave conculcación, entre otros, del principio de proporcionalidad[281].

IV.2.- Aplicación del secreto de las comunicaciones a las distintas manifestaciones de intercambio automático de datos a través de redes de comunicaciones electrónicas. Enfoque desde el punto de vista del Derecho de la Unión Europea

[281] El ejemplo de la legislación británica anterior a la *Regulation Investigatory Powers Act* de 2000, puede ser claro ejemplo de ello, a nivel del establecimiento de técnicas de control preventivo por parte de los poderes públicos. Baste con analizar las SSTEDH de 1 de julio de 2008 (caso Liberty y otros *vs.* Reino Unido; asunto núm. 58243/2000), y de 18 de mayo de 2010 (caso Kennedy *vs.* Reino Unido; asunto núm. 26839/05).

La libertad de comunicaciones se entiende en un escenario jurídico en el que solamente por decisión judicial podrá accederse a aquello que incumbe únicamente a los interlocutores y que encuentra una férrea protección basada en un concreto deber de confidencialidad exigible a aquel en quien se confía el tránsito de la comunicación durante el tiempo que dependa de él.

La voluntariedad e intervención humana es predicable de una comunicación que editamos y transmitimos personalmente e incluso, de aquellas informaciones que, si bien circulan por las redes de forma automática, son consecuencia directa o están íntimamente ligadas a una actuación voluntaria nuestra (la actualización de un perfil accesible a un número reducido de personas o de información asequible en *gadgets,* puede generar de forma automática notificaciones de cambios de estado, eventos,…). Sin embargo, cuando hablamos de comunicaciones respecto de las que bien, simplemente, somos completamente ajenos, al no tener con ellas más relación que la de ser titulares o usuarios de determinado dispositivo electrónico, o bien obedecen a pautas de actuación objeto de una previa programación o diseño, disociándose claramente del componente decisorio humano, la búsqueda de una solución incontestable se nos antoja realmente compleja, como así afirma RODRÍGUEZ LAÍNZ[282].

[282] RODRÍGUEZ LAÍNZ, J. L., *Internet de los objetos…*, *op. cit.*

En este sentido, analizando el artículo 18 de la Constitución Española y la jurisprudencia al respecto, se podría afirmar que quedan fuera de la protección otorgada por el derecho al secreto de las comunicaciones, todos los diálogos automáticos generados para la gobernanza de dispositivos electrónicos y ello, por cuanto no transmiten, ni directa ni indirectamente, ningún tipo de contenido en el que intervenga la voluntad humana, como sería el caso de la información que manejan terminales telefónicos, *smartphones* o dispositivos de localización para su actualización, a efectos de su correcto funcionamiento o prestación de servicios con valor añadido, la actualización automática de *gadgets*, *hardware* o *software*, o la ejecución de programas antivirus a través de la llamada inteligencia colectiva (*cloud computing*).

Una mayor dificultad plantearía la transmisión de información encaminada a su gestión automatizada al servicio no del funcionamiento interno de un dispositivo o un sistema de dispositivos, sino de una finalidad diversa en la que sí interviene directa o indirectamente el ser humano, por cuanto representa una estructurada programación de respuestas automáticas que obedecen a unos criterios que sí serían representación de ideas o manifestaciones de voluntad de personas físicas o jurídicas. Por ejemplo, el registro de salidas de existencias de un almacén o establecimiento que, transmitido por radiofrecuencia a un receptor, es enviado a un servidor central, el cual está programado para generar decisiones sobre destinos de stocks, entiende RODRÍGUEZ LAÍNZ

que sí podría, en este sentido, considerarse una comunicación, y respondería a ese concepto de voluntariedad y transmisión de contenidos entre personas, como verdaderamente sustitutiva de una comunicación entre personas.

Sin embargo, los restantes y escasos autores, que han tratado tangencialmente esta materia, se muestran reticentes a otorgar dicha protección. GONZÁLEZ LÓPEZ[283], por ejemplo, habla de que si bien podría intentar sostenerse que indirectamente existen dos interlocutores personales en el supuesto de terminales de telefonía móvil: el usuario del terminal y el operador al que corresponde la estación base, existe un argumento, el de la finalidad de estas comunicaciones técnicas, que nos conduciría a negar la inclusión apuntada. La misma reticencia se puede inferir de la Circular de la Fiscalía General del Estado 1/2013 al defender que *"las comunicaciones comprendidas en este derecho han de ser aquellas indisolublemente unidas por naturaleza a la persona, a la propia condición humana"*.

Enfoque desde el punto de vista del Derecho de la Unión Europea

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas

[283] GONZÁLEZ LÓPEZ, J. J., *Obtención de la IMSI con fines de investigación penal…, op. cit.*

-*Directiva sobre la privacidad y las comunicaciones electrónicas*[284]- se fija únicamente en la información generada con motivo de la prestación de servicios de comunicaciones electrónicas (y encajaría a la perfección en ese concepto de la gobernanza de determinados dispositivos electrónicos a través de diálogos automáticos que circulan por las redes de telecomunicaciones), en tanto en cuanto interesa para garantizar que la misma solamente deba o pueda ser objeto de almacenamiento y tratamiento en el contexto de la prestación del concreto servicio al que atienden.

Así plasma la necesidad de evitar el acceso no autorizado a las comunicaciones[285], a fin de proteger la confidencialidad de las mismas, incluyendo, tanto sus contenidos como cualquier dato relacionado con ellas, por medio de las redes públicas de comunicaciones y los servicios de comunicaciones electrónicas disponibles al público; no permite su almacenamiento ni el de los datos de tráfico relativos a éstas, por terceros distintos de los usuarios o sin su consentimiento[286], dejando claro que su

[284] Artículos 5.1 y .3, 6.1 y .3 y 9.1 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas -*Directiva sobre la privacidad y las comunicaciones electrónicas*-, DOUE, núm. 201, de 31 de julio de 2002.

[285] Conforme a la Directiva 2002/58/CE, una comunicación puede incluir cualquier dato relativo a nombres, números o direcciones facilitado por el remitente de una comunicación o el usuario de una conexión para llevar a cabo la comunicación. Los datos de tráfico pueden incluir cualquier conversión de dicha información efectuada por la red a través de la cual se transmita la comunicación a efectos de llevar a cabo la transmisión. Los datos de tráfico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión. También pueden referirse al formato en que la red conduce la comunicación.

[286] Artículo 5.1 y 5.3 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la

finalidad no es prohibir el almacenamiento automático, intermedio y transitorio de esta información, en la medida en que sólo tiene lugar para llevar a cabo la transmisión en la red de comunicaciones electrónicas y siempre que la información no se almacene durante un período mayor que el necesario para la transmisión y para los fines de la gestión del tráfico, y que durante el período de almacenamiento se garantice la confidencialidad.

Por tanto, la confidencialidad está garantizada realmente respecto de lo que son contenidos o datos de tráfico de comunicaciones electrónicas en las que intervienen los usuarios, quedando el resto de la información exclusivamente bajo un deber de confidencialidad ajeno al

---

protección de la intimidad en el sector de las comunicaciones electrónicas -*Directiva sobre la privacidad y las comunicaciones electrónicas*-: *"1. Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad. […]*

3. Los Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento. La presente disposición no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado".

Articulo 6.1 de la anterior Directiva: *"Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación".*

concepto mismo de comunicación. De hecho, la STJUE, Sala Tercera, de 22 de noviembre de 2012 (asunto -119/12), no ve reparo jurídico alguno en la cesión de datos de facturación de llamadas telefónicas (lo que incluye información detallada de tráfico de llamadas) para su gestión de cobro; con la única exigencia de que el cesionario actúe bajo el control de la operadora cedente y de que también se comprometa a realizar un tratamiento lícito de tales datos.

Como vemos, la anterior Directiva nada nos aclara al respecto del intercambio automático de información y de su configuración jurídica.

Aún es más, tampoco lo hace la posterior Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones[287], la cual se limita a distinguir entre datos de tráfico y datos relativos a las comunicaciones, entre los que se encontrarían la localización de personas físicas o jurídicas y los necesarios para identificar al abonado o usuario registrado[288].

[287] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, DOUE, núm. 105, de 13 de abril de 2006.

Esta Directiva 2006/24/CE ha sido recientemente anulada por la STJUE, Gran Sala, de 8 de abril de 2014 debido a la escasa definición en la norma de las cautelas y garantías jurídicas precisas y claras que exige la inmisión en el derecho a la protección de datos personales.

[288] Artículo 1.2 de la citada Directiva: *"La presente Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado".*

Tampoco las instituciones comunitarias aportan mucho a la materia. La Comisión, en su Comunicación de 18 de junio de 2009, dedicada a "Internet de los objetos-plan de acción para Europa", no se plantea más objetivo a corto y medio plazo que el de garantizar la seguridad de la información que transita por la red; entendiendo por seguridad de la información, no tanto la garantía del libre tránsito ajeno a inmisiones por parte de terceros, como una protección de la información relevante que pueda contener o una garantía frente al mal tratamiento de la información que podría dar lugar a la revelación de datos personales o comprometer la confidencialidad de datos empresariales.

Más destacable es el Dictamen del Supervisor Europeo de Protección de Datos[289] acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad —2010/C 280/01— al plantear como preocupación en relación a la IO (Internet de los Objetos), no solo los riesgos del almacenamiento y tratamiento no consentidos de datos de carácter personal, sino también la información que puede circular sobre aspectos relevantes de la intimidad de las personas pudiera ser rastreada sin

[289] La figura del Supervisor Europeo de Protección de Datos (SEPD) se creó en 2001. El SEPD tiene la responsabilidad de garantizar que las instituciones y organismos de la UE respeten el derecho de las personas a la intimidad en el tratamiento de sus datos personales.
SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS. Recuperado de: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS?lang=es (última consulta: 9 de diciembre de 2015).

restricciones por terceros que pudieran acceder a la información facilitada por etiquetas RFID.

IV.3.- Protección de las comunicaciones ya finalizadas

Obtener información sobre estado de activación o identidad del terminal (números IMSI e IMEI) o acceder a la información que comparten estaciones BTS y determinados terminales, para posicionar un determinado teléfono móvil independientemente de la emisión o recepción de comunicaciones[290], es ya posible, como hemos explicado, mediante técnicas de interceptación de señales o de interactuación o monitorización remota a través de falsas BTS interpuestas.

Asimismo podríamos realizar barridos de señales emitidas por etiquetas asociadas a objetos, para, por ejemplo, realizar su seguimiento, pero evidentemente, el acceso a la información que pueden facilitar estos

[290] Ya la sentencia del Tribunal Supremo, Sala Segunda, 777/2012, de 17 de octubre, analizó y trató la información almacenada respecto de determinadas estaciones BTS. Así afirmó que ninguna vulneración puede predicarse de la utilización de un método que lo único que pretende es conseguir, en un radio de acción prefijado, la activación de unos mecanismos de comunicación, traducidos en números, de donde pueda inferirse la localización de unos terminales de donde inducir la presencia de unos pocos sospechosos que respondan a la utilización más certera de un material que se ha conseguido por otros medios probatorios y que, como hemos visto, se han obtenido a través de informaciones directas, comprobables y legítimas. Y en este sentido el Tribunal Supremo ya ha declarado que cuando *"esa ubicación sólo puede concretarse con una aproximación de varios cientos de metros, que es la zona cubierta por la BTS o estación repetidora que capta la señal, en modo alguno puede considerarse afectado, al menos de forma relevante, el derecho a la intimidad del sometido a la práctica de la diligencia"* (Sentencia del Tribunal Supremo, Sala Segunda 906/2008, de 19 de diciembre). En el misma línea, la sentencia del Tribunal Supremo, Sala Segunda, 706/2006, de 14 de junio.

dispositivos electrónicos lo será normalmente una vez que estas comunicaciones se han consumado y, en tanto en cuanto, permanezcan almacenadas, bien en bases de datos a disposición de los prestadores de servicios, bien del contenido de los propios dispositivos que pudieran ser objeto de incautación.

Aunque todos estos diálogos automáticos quedarían fuera del ámbito de protección del derecho al secreto de las comunicaciones, se plantea RODRÍGUEZ LAÍNZ[291] que, tanto si pretendemos extender tal protección a estos diálogos, como si reservamos tal consideración al flujo de información directa o indirectamente relacionada con determinadas manifestaciones de voluntad del ser humano, surge el problema de si tal protección constitucional habría de mantenerse, más allá del tránsito de la comunicación, una vez consumada esta.

Recuerda el autor que si bien la posición inicial del Tribunal Constitucional se definió de forma inequívoca hacia la idea de pérdida de protección formal una vez que la comunicación había sido consumada[292], el salto cualitativo hacia la perpetuación de la protección formal más allá del tránsito de la comunicación, vendría de la mano de la sentencia del Tribunal Constitucional 230/2007, de 5 de noviembre, siendo el

[291] RODRÍGUEZ LAÍNZ, J. L., *Internet de los objetos…*, *op. cit.*
Se reproduce el análisis del autor al respecto de la cuestión planteada por considerarse del todo excelente.

[292] Sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre, seguida por las posteriores sentencias 70/2002, de 3 de abril, y 123/2002, de 20 de mayo, que defienden que la protección de las comunicaciones ya consumadas pasaría a ser *"…a través de las normas que tutelan la intimidad u otros derechos"*.

auténtico factor desencadenante de tan radical cambio de criterio la casi contemporánea STEDH de 3 de abril de 2007 (caso Copland *vs.* Reino Unido; asunto 62617/00). Así, realizando un estudio comparativo del caso Copland, concluye que la protección formal va más allá de la finalización de la comunicación, perpetuándose; de suerte que cualquier acceso no consentido por emisor, destinatario o interlocutor, o que no contara con una previa autorización judicial, supondría una vulneración del artículo 18.3 de la Constitución Española.

Posteriormente la sentencia del Tribunal Constitucional 142/2012, de 2 de julio, plasma un escenario caótico, dado que si bien la sentencia parece reconocerse heredera de la sentencia del Tribunal Constitucional 230/2007, de 5 de noviembre, en cuanto respecta a la perpetuación de la protección formal del secreto de las comunicaciones, introduce nuevos parámetros que acercan claramente a tal institución a la protección genérica del derecho a la intimidad, a través principalmente de la relativización del concepto mismo del poder de exclusión, mediante la instauración del principio de la expectativa razonable de confidencialidad, y de la quiebra que supone la posibilidad de accesos lícitos basados en lo que generosamente define como hallazgo casual; y a su vez, vuelve a recordarnos la vigencia del criterio jurisprudencial de la mutación de la naturaleza de lo comunicado, una vez la comunicación se consuma.

Pero ni la sentencia del caso Malone ni la del caso Copland pretenden bajo ningún concepto extender la protección formal del secreto de las comunicaciones más allá de la garantía de su libre tránsito ajeno a

injerencias externas. La primera sentencia, de hecho, analiza realmente un supuesto de captación en origen, mediante la utilización de dispositivos analógicos de recuento; la segunda cuestiona fundamentalmente la utilización abusiva de información referente a facturación de llamadas, cuyo acceso lícito para el empresario era incuestionable y el examen de archivos temporales de Internet almacenados en el PC utilizado por una empleada; este planteamiento no responde a otra cosa que a la prohibición de excesividad en la utilización de datos de carácter personal cedidos al titular de la línea telefónica para una finalidad específica, que no es la de controlar a una empleada que habría visto afectada su intimidad en el ámbito laboral por el hecho de haber sido objeto de inspección en el ámbito del rastro de sus comunicaciones, sin su previo conocimiento ni consentimiento. Si en el primer ejemplo el TEDH llega incluso a justificar el acceso y conservación de datos de tráfico, por parte de operadoras de comunicaciones a los efectos de la prestación de su servicio y de facturación, en el segundo, realmente, nos estamos enfrentando a una de las dimensiones del derecho al respeto de la correspondencia que trasciende al secreto mismo.

Examinando, de hecho, otras resoluciones de nuestro TEDH, podemos comprobar con facilidad cómo la equiparación entre nuestro derecho al secreto de las comunicaciones con el derecho al respeto de la correspondencia no es precisamente de paridad. La segunda considera a la primera como una simple parte de un todo y ello incluso sin tener que

acudir a la visión global del concepto de privacidad que defendiera en trabajos anteriores. Las STEDH de 24 de agosto de 1998 (caso Lambert *vs.* Francia, asunto 23618/1994), y de 29 de marzo de 2005 (caso Matheron *vs.* Francia, asunto 57752/2000) apuntan a la existencia de una transgresión del derecho al respeto de la correspondencia, no por una vulneración de un secreto en el contexto de un acto de injerencia acordado en otro procedimiento, sino en la falta de vías procesales efectivas que permitieran a las personas afectadas cuestionar la licitud de las medidas adoptadas. Pero si en un cuerpo de resoluciones podemos apreciar esa concepción amplia de la correspondencia, como objeto de protección más allá de la garantía del secreto, será sin duda con la línea abierta por la STEDH de 16 de octubre de 2007 (caso Wieser y Bicos Beiligungen GMBH *vs.* Austria; asunto 74336/01); seguida por las SSTEDH de 22 de mayo de 2008 (caso Ililla Stefanov *vs.* Bulgaria; asunto núm. 65755/01), y, Secc. 1ª, de 22 de diciembre de 2008 (caso Aleksanyan *vs.* Rusia; asunto 46468/06). La primera de las sentencias citadas, de hecho, podría parecer llevarnos a equívoco cuando de forma tan rotunda nos dice que *"...la búsqueda e incautación de datos electrónicos constituye una interferencia del derecho de los interesados al respeto de su correspondencia dentro del ámbito del art. 8".,* pero si analizamos con detenimiento la sentencia, descubriremos cómo el Alto Tribunal no ya no se detiene en declarar la existencia del acto de injerencia sobre el secreto de las comunicaciones por razón de la incautación policial y examen del disco duro de un PC de asesoría jurídica de empresa farmacéutica, en el contexto de un registro de sede

de asesoría jurídica, sino que se limita a analizar el conflicto en términos de proporcionalidad, relacionando el factor tiempo de la retención del dispositivo de almacenamiento con la finalidad de búsqueda pretendida, y la especial naturaleza de parte de los contenidos como relacionados con servicios jurídicos de una empresa. Esta visión se verá aún más clara si tenemos en cuenta la más reciente STEDH, Sección 1ª, de 3 de julio de 2012 (caso Robathin *vs.* Austria; asunto 30457/06), donde, pese a que en ningún momento reconozca que las carpetas de clientes del abogado contuvieran contenidos o rastros de comunicaciones electrónicas, se advierte que el acceso a la información contenida en el disco duro suponía igualmente una injerencia en su derecho al respeto de su correspondencia.

No otra explicación puede tener, por otra parte, la diferenciación que en la legislación comunitaria se hace entre contenidos y datos de tráfico o relativos a las comunicaciones, a la hora de regular el artículo 1.2 de la Directiva 2006/24/CE la obligación de retención de datos por parte de las operadoras. Se excluyen taxativamente lo que se denominan contenidos; a la vez que se reconoce una plena adaptación al CEDH y a la jurisprudencia que lo interpreta. Menos la falta de sensibilidad con que la STJUE, Sala Tercera, de 22 de noviembre de 2012 se enfrenta a lo que no sería una transgresión del vínculo de confidencialidad entre cliente y operadora: nada más y nada menos que la cesión de los datos de tráfico por ella almacenados para su gestión de cobro por un tercero.

Por ello, la solución anticipada por la pionera sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre, residenciando la protección constitucional de lo comunicado (y debe entenderse igualmente de su rastro electrónico), no ya en el ámbito del secreto de las comunicaciones, sino de la protección de la intimidad o de los datos de carácter personal, no puede ser más conforme con la doctrina del TEDH. Lo que para la jurisprudencia del TEDH sigue siendo respeto de la correspondencia, para nuestro ordenamiento constitucional pasaría a ser intimidad/protección de datos de carácter personal.

Todo lo anterior es lo defendido por RODRÍGUEZ LAÍNZ, ya que desde que nace en el emitente y en el destinatario la posibilidad real y efectiva de conservar o eliminar o destruir ese contenido o rastro, se pierde la protección formal, pasando a depender de esos otros ámbitos de la privacidad.

V.- SISTEMA SILENT

Como ya se avanzó en el capítulo anterior, este sistema de geolocalización se articula a través del envío, por parte de las unidades de investigación, de un mensaje *SMS* al dispositivo móvil que pretenden situar, mensaje que no es recibido por su usuario desconociendo éste ,por tanto, que está siendo rastreada su ubicación.

Si bien estos *SMS* son archivados por las operadoras de telecomunicaciones como acto de comunicación, ello es así considerado desde un punto de vista técnico, lo cual no debe conducirnos a esa misma conclusión en el ámbito jurídico.

Los mensajes emitidos a través del sistema *Silent* no afectan al derecho al secreto de las comunicaciones reconocido en el artículo 18.3 Constitución Española sino, en todo caso, a la intimidad y al derecho a la protección de datos personales del usuario del dispositivo. Estos mensajes no gozan de las características propias de un proceso comunicativo y se acercarían más a una catalogación de los mismos pareja a los datos IMSI e IMEI, debiéndose recordar a este respecto la meritoria sentencia del Tribunal Supremo, Sala Segunda, 249/2008, de 20 de mayo, FJ4, la cual defiende la no inclusión de todos los datos de tráfico de manera automática en el ámbito de protección reforzado del secreto de las comunicaciones, dejando a un lado del mismo, actualizando la pauta interpretativa ofrecida por el TEDH, todos aquellos que no sean datos indicativos del origen y del destino de la comunicación, del momento y duración de la misma o, por último, los referentes al volumen de la información transmitida y el tipo de comunicación entablada.

Así, la negación del carácter de dato integrable en el contenido del derecho al secreto de las comunicaciones, no implica su irrelevancia constitucional que, por contra, sí la ostenta en relación al artículo 18.4

de la Constitución Española como dato personal digno de protección frente al uso de la informática.

VI.- ARCHIVOS EXIF

El descubrimiento de los datos de geolocalización, a través de los archivos *Exif,* puede suponer una injerencia en diversos derechos constitucionales dependiendo del origen de dicho archivo dentro del dispositivo electrónico.

Si el usuario hubiera incluido dicho archivo dentro de un proceso comunicativo, todo él y, por tanto, también los datos de geolocalización en el mismo incluidos, revestirían la calificación de comunicación y estaríamos, en el supuesto de su intervención, dentro de la protección reforzada del artículo 18.3 Constitución Española o del secreto de las comunicaciones.

Si dicho archivo formó parte de un proceso comunicativo ya finalizado, y la conservación del mismo por el interlocutor dentro del dispositivo electrónico forma parte de una decisión autónoma y voluntaria del individuo, solo merecería la protección otorgada por el derecho a la intimidad, por encontrarnos ante una simple información conservada en soporte informático; esta posición se fundamenta en la sentencia del Tribunal Constitucional 142/2012, de 2 de julio, que

plantea si el acceso a la agenda del teléfono por agentes es un acto administrativo sólo con incidencia en el derecho a la intimidad, o alcanza también al derecho al secreto de las comunicaciones. Pues bien, a la vista de la anterior resolución, el hecho de que la agenda, en nuestro caso sería una fotografía, tenga su ubicación en un terminal telefónico móvil, que es un instrumento de y para la comunicación, no condiciona el carácter que tiene dicha información entendiendo que, en todo caso, se vería afectado el derecho a la intimidad del usuario del dispositivo en aplicación de la doctrina de la expectativa razonable de confidencialidad[293].

Lo mismo ocurriría si dicho archivo *Exif* se encuentra en el terminal electrónico dentro de su memoria como cualquier otro dato que el usuario guarda en el dispositivo, ajeno a cualquier comunicación. Su uso para el descubrimiento de datos de geolocalización afectaría al derecho a la intimidad del usuario, sobre la base del artículo 18.1 de la Constitución Española, pero nunca más allá[294].

---

[293] Incluso antes, las sentencias del Tribunal Supremo, Sala Segunda, 1235/2002, de 27 de junio, y 1647/2002, de 1 de octubre, postularon la no afectación al derecho al secreto de las comunicaciones por el acceso policial al contenido de memorias de teléfonos móviles, tanto respecto de datos de tráfico (llamadas emitidas y recibidas), como de mensajes ya recibidos y a los que tuvo previo acceso el encartado. Estas resoluciones consideran que los mensajes de teléfonos móviles participan de la condición de comunicaciones telefónicas, y perderían tal cualidad cuando la comunicación misma se ha consumado, entrando ya en juego la esfera de la protección de la intimidad y, por ende, la posibilidad de que las unidades policiales, en casos excepcionales, y por razones de urgencia, puedan acceder al contenido de tales memorias para recabar datos de comunicaciones recientes o contenidos de mensajes almacenados.

[294] La sentencia del tribunal Supremo, Sala Segunda, 1231/2003, de 25 de septiembre analiza el caso de funcionarios del servicio de vigilancia aduanera que intervinieron tres terminales móviles, los cuales manipularon para acceder, en la memoria del teléfono, a los datos sobre las llamadas realizadas y recibidas, y la localización de los números con los que los detenidos se habían comunicado. Esta

Lo anterior es avalado por la línea jurisprudencial, así la sentencia del Tribunal Supremo, Sala Segunda, 1315/2009, de 18 de diciembre, la cual, aparte de dar el tratamiento diferenciado al contenido de agendas de teléfonos móviles, amparadas tan solo por la protección del derecho a la intimidad, y por tanto, vulnerables a inspecciones policiales en el supuesto en que la medida resultara justificada y proporcional, asume hasta las últimas consecuencias la doctrina sentada por el precedente de la sentencia del Tribunal Constitucional 70/2002, de 3 de abril, y concluye, mas concretamente que el acceso por los agentes de la Guardia

---

sentencia defiende, apoyándose en sentencias anteriores tales como 316/2000, de 3 de marzo ,1235/2002 de 27 de junio, y 1086/2003 de 25 de julio, y usando el discurso jurídico de la sentencia del Tribunal Constitucional 70/2002, de 3 de abril, la legitimidad de la indagación en la memoria del aparato móvil de telefonía, equiparando la agenda electrónica del aparato de telefonía con cualquier otra agenda en la que el titular puede guardar números de teléfonos y anotaciones sobre las realizadas y llamadas y otras anotaciones que, indudablemente, pertenecen al ámbito de la intimidad constitucionalmente protegida y que admiten injerencias en los términos exigidos por el articulo 8 del CEDH y la Constitución, *"pues no tiene la consideración de teléfono en funciones de transmisión de pensamientos dentro de una relación privada entre dos personas"* (FJ8), añadiendo que *"esta diligencia [el listado de llamadas del móvil] no supone ninguna intromisión en el derecho a la intimidad, ya que han sido obtenidas en legal forma y sólo sirven para acreditar los usuarios de los teléfonos intercomunicados, sin entrar en el contenido de las conversaciones".* Dentro de la no vulneración del derecho al secreto de las comunicaciones, y su traslado a una posible afectación al derecho de intimidad, la resolución tampoco consideró la existencia de daño alguno del principio de proporcionalidad en el hecho de que las unidades de policía judicial se anticiparan en el acceso a tales datos, por las necesidades perentorias de la propia averiguación de los hechos, y sobre todo para la evitación de la fácil destrucción o inutilización del contenido informativo de tales memorias.

Para RODRÍGUEZ LAÍNZ el mayor mérito de esta sentencia (STS 1231/2003) radica en el reconocimiento de una especie de principio de disponibilidad del objeto de la injerencia del que llega a deducir, implícitamente, una especie de presunción de renuncia tácita a la protección constitucional del dato bajo el manto del secreto de las comunicaciones, al defenderse en la resolución (FJ8) que *"se trata de una comprobación de una agenda que contiene datos almacenados y que pudieron ser borrados por el titular o, incluso, bloqueados por el titular"*. Si el dato de tráfico o el contenido de la información se transmutan en simple información amparada tan solo por el derecho a la intimidad de su titular, y como tal desvelable por una actuación policial en situaciones de urgencia, y el titular no decide su borrado o bloqueo, estaría asumiendo éste el riesgo de su vulnerabilidad a un lícito acceso en el curso de una detención policial. Con más motivo, la colaboración del detenido mostrando el número que aparece en pantalla para facilitar la detención de su proveedor de drogas, o incluso manteniendo conversación con éstos, nada tendría que objetar en cuanto a su licitud.

Vid., RODRÍGUEZ LAÍNZ, J.L., *Incautación policial de teléfonos móviles y secreto de las comunicaciones*, Diario La Ley, núm. 7536, Sección Doctrina, Ref. D-407, Año XXXI, Editorial LA LEY, 28 de diciembre del 2010, p. 7.

Civil al archivo del teléfono móvil donde se contiene la "agenda" o "números telefónicos de los contactos", sin autorización judicial, no es una vulneración del derecho al secreto de las comunicaciones, sino todo lo más, del derecho a la intimidad del investigado, lo cual no requiere de previa autorización judicial, más al contrario la diligencia que afecta a la intimidad del investigado se encuentra legalmente autorizada a las fuerzas del orden (artículo 282 de la Ley de Enjuiciamiento Criminal, artículo 11.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de seguridad del Estado y artículo 14 de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana), siempre, por supuesto, que la misma resulte justificada y proporcional[295].

[295] Sentencia del Tribunal Constitucional 70/2002, de 3 de abril: "*c) A la vista de la doctrina anteriormente expuesta, en el presente caso, si la carta hallada por la Guardia Civil en el momento de la detención hubiera tenido inequívocamente tal carácter, podríamos plantearnos si estaríamos en el ámbito de protección del artículo 18.3 de la Constitución Española.*

Sin embargo, el hallazgo que se produce es algo distinto. Pues la supuesta carta no presentaba ninguna evidencia externa que hubiera permitido a la Guardia Civil «ex ante» tener la constancia objetiva de que aquello era el objeto de una comunicación postal secreta, tutelada por el artículo 18.3 de la Constitución Española. Por el contrario, la apariencia externa del hallazgo era equívoca: unas hojas de papel dobladas en el interior de una agenda no hay por qué suponer que fueran una carta y no resultaría exigible a la Guardia Civil que actuara respecto de cualquier papel intervenido al delincuente, en el momento de la detención, con la presunción de que se trata de una comunicación postal.

A lo que ha de añadirse otra consideración, relativa al momento en que se produce la intervención policial. Pues tal intervención no interfiere un proceso de comunicación, sino que el citado proceso ya se ha consumado, lo que justifica el tratamiento del documento como tal (como efectos del delincuente que se examinan y se ponen a disposición judicial) y no en el marco del secreto de las comunicaciones. La protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos."

VII.- VIGILANCIA DISCRETA -BALIZAS-

Como ya se ha explicado anteriormente las balizas son una modalidad dinámica de localización usada por las Fuerzas y Cuerpos de Seguridad del Estado. Con ellas se controla de forma permanente los movimientos que realiza una persona a través de la señal enviada por un dispositivo colocado en el entorno del sujeto monitorizado.

Su ventaja y proliferación en su uso proviene no solo de que es una herramienta de enorme utilidad en la propia investigación[296], sino que su utilización supone, ciertamente, un considerable ahorro de costes de personal.

En el ámbito europeo, la sentencia TEDH, de 2 de septiembre de 2010, caso UZUN *vs.* Alemania, en un supuesto de intervención de una cabina telefónica habitualmente usada por un supuesto terrorista, si bien consideró que tal vigilancia a través del sistema GPS, y procesamiento de los datos obtenidos constituía una injerencia en la vida privada, art. 8 Convenio, también precisó que la vigilancia GPS, por su propia naturaleza debe distinguirse de otros métodos de seguimiento acústico o visual que, por regla general son más susceptibles de interferir en el

[296] VALLÉS expone que "*este medio técnico es, en general, un sistema auxiliar en la investigación que no sustituye en modo alguno a los procedimientos policiales clásicos, como las vigilancias o los seguimientos, y que aporta un suplemento de seguridad y eficiencia en el control de unos objetivos que pueden acceder con gran comodidad a los medios de transporte, a veces muy rápidos, o que viajan fuera del alcance del seguimiento directo en rutas extraterritoriales por tierra, mar o aire*".

Vid., VALLÉS CAUSADA, L. M., "La policía judicial en la obtención de inteligencia…", *op. cit.*, p.403.

derecho de la persona al respeto de su vida privada, porque revelan informaciones sobre la conducta de una persona, sus operaciones o sus sentimientos.

En dicha línea, también se ha pronunciado una reciente sentencia del Tribunal Supremo de EE.UU. [*U.S. vs. Jones,* 565 U.S. (2012)], al afirmar que sí se afecta a una expectativa razonable de privacidad *(reasonable expectation of privacy)*[297]cuando se instala un sistema GPS a un individuo al que se está realizando un seguimiento en una investigación criminal.

La jurisprudencia española sobre esta materia es escasa. Desde una primera sentencia del Tribunal Supremo, Sala Segunda, 562/2007, de 22 de junio, que defendía la no afectación de derecho fundamental alguno, por lo que su uso no precisaba de autorización judicial, se evolucionó hacia la sentencia 906/2008, de 19 de diciembre, que ya sí preveía una posible vulneración de la intimidad si la utilización de este instrumento permitiera "conocer el lugar exacto en el que el comunicante se encontraba".

[297] El embrión de esta teoría reside en *Katz vs. United States,* 389 U.S. 347 (1967). Así, de acuerdo con el razonamiento judicial contenido en esta conocida decisión judicial, el modo de verificar *(litmus test)* la concurrencia de una tal *reasonable expectation of privacy* se debía realizar con base en dos estándares: (1) el sujeto debía tener una expectativa real de privacidad en la situación en la que se produjeron los hechos *(dimensión subjetiva);* y (2) la sociedad debe estar predispuesta para reconocer tal expectativa como razonable *(dimensión objetiva).* La decisión que dio la razón al particular se fundamentó en que el acusado tenía la expectativa razonable de privacidad cuando realizaba las llamadas telefónicas, pudiendo esperar que no serían interceptadas por la policía o el FBI, y que la sociedad compartía esa expectativa.

Relevante es en esta materia la sentencia del Tribunal Supremo, Sala Segunda, 798/2013, de 5 de noviembre, que clarifica la posición del Alto Tribunal en relación con el uso de estos dispositivos, así ha de entenderse que las balizas de seguimiento GPS no vulneran el derecho fundamental al secreto de las comunicaciones ni suponen una inferencia excesiva sobre el derecho fundamental a la intimidad a los efectos de exigir un control jurisdiccional previo y una ponderación sobre dicha afectación constitucional.

La ausencia de relevancia constitucional se deriva de que se trata de "diligencias de investigación legítimas 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"[298].

Sin embargo, para autores como VELASCO[299], la privacidad no debe analizarse desde una perspectiva meramente locativa (de lo que es ejemplo la afirmación *"la calle es pública, y los domicilios, privados"*), sino desde una doble consideración, así su dimensión objetiva o la de lo que socialmente se admite como íntimo según las circunstancias concurrentes y su dimensión subjetiva, o lo que el afectado quiso excluir con su concreta actitud. Por lo anterior, defiende la validez probatoria de este método de vigilancia únicamente cuando se complemente y

[298] Sentencias del Tribunal Supremo, Sala Segunda, de 22 de junio de 2007, de 11 de julio de 2008, de 19 de diciembre de 2008.

[299] VELASCO recuerda la sentencia del Tribunal Supremo de EE.UU. *Katz vs. US,* 389 US 347 (de) 1967 cuando señala que: "la 4ª enmienda protege personas, no sitios".

Vid., VELASCO NÚÑEZ, E., *Tecnovigilancia, geolocalización y datos…*, *op. cit.*

corrobore con seguimientos policiales convencionales, entendiendo que si la colocación de la baliza es para una actuación ocasional, puntual, no exige mandamiento judicial, dada su apenas despreciable intrusión, mientras que sí existe afectación de la vida privada del investigado y su "expectativa razonable de privacidad", si su colocación es sobre un terminal de uso privado, como portátil o móvil, su uso muy intenso (por ejemplo dilatado en el tiempo), afectando a espacios públicos y privados.

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, prevé la utilización de esta medida en el artículo 588 quinquies b, siempre que concurran acreditadas razones de necesidad y resulte proporcionada, existiendo previa autorización judicial al respecto con carácter general, si bien por razones de urgencia que hagan razonablemente temer que de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y localización se frustrará la investigación, la Policía Judicial podrá proceder a su colocación, dando cuenta a la mayor brevedad posible y, en todo caso, en el plazo máximo de 24 horas a la autoridad judicial, quien podrá ratificar la medida adoptada o acordar su inmediato cese. Para este último supuesto, la información obtenida a partir de la baliza colocada carecerá de efectos en el proceso.

La duración de la medida será de tres meses como máximo a partir de la fecha de autorización, aunque excepcionalmente el Juez podrá prorrogar su uso por el mismo o inferior plazo hasta un máximo de dos años, si así estuviera justificado, a la vista de los resultados obtenidos.

A juicio de la autora de esta investigación, es una medida equiparable a la del seguimiento tradicional, con las diferencias propias de su configuración tecnológica. En su uso ha de respetarse el principio de proporcionalidad, entendido en sus dimensiones de adecuación, necesidad y proporcionalidad en sentido estricto. El necesario dictado de resolución judicial autorizante nos lleva al absurdo de permitirse sin autorización judicial los seguimientos físicos tradicionales y, sin embargo, los efectuados a través de balizas, por el simple mero hecho de que es un "seguimiento tecnológico", necesita de mayores garantías (a pesar de su equivalencia)[300].

Como se ha visto, dependiendo del tipo de herramienta tecnológica usada y del modo de obtención y /o intervención, estamos ante datos de geolocalización que ostentan naturaleza jurídica distinta, la cual nos orienta para la necesaria determinación de la norma aplicable y la deducción de las exigencias legales a cumplir.

[300] Comparto plenamente la posición de VALLÉS quien afirma que *"el uso de balizas reduce los periodos de exposición de los vigilados a aquellos sucesos ajenos al interés del proceso penal y, consiguientemente, presentan unas ratios muy bajas, e incluso irrelevantes si se comparan con otros medios de investigación, de penetración en el derecho a la intimidad".*

Vid., VALLÉS CAUSADA, L. M., "La policía judicial en la obtención de inteligencia…", *op. cit.*, p. 404.

La geolocalización como hemos visto ostenta una pluridimensionalidad, y no puede ser tratada desde una sola línea, dado que las variantes son muchas en la actualidad y más serán con el tiempo y el desarrollo de la tecnología, mereciendo cada una de ellas una particular previsión legal acorde a su naturaleza jurídica, dependiendo de los derechos afectados, y siempre en pos de la más que exigible seguridad jurídica que debe ampararnos como ciudadanos.

Una vez que los datos se han obtenido y/o intervenido con pleno respeto a la legalidad que impera, hemos de valorar la utilidad de dichos datos dentro del proceso penal y su conversión de fuente de prueba a medio de prueba, cuestión de la que se trata en el capítulo siguiente.

CAPÍTULO III

TRATAMIENTO DE LOS DATOS DE GEOLOCALIZACIÓN EN EL PROCEDIMIENTO PENAL

Partiendo de la pluridimensionalidad de los datos de geolocalización, y habiendo obtenido una clara visión en cuanto a su forma de obtención y/o intervención de manera legal y respetuosa con la intimidad y el derecho al secreto de las comunicaciones, en relación con la naturaleza jurídica de cada uno de ellos, intentamos, en este capítulo, saber su utilidad procesal y, además, queremos conocer cómo se deben convertir de fuente a medio de prueba en el proceso penal.

I.- INTRODUCCIÓN

Se hace necesario plantear de manera sucinta las fases del procedimiento penal[301]; la primera fase, la de instrucción, determina la existencia de un posible hecho punible y la presunta participación en el mismo de uno o varios imputados, concluyendo con la acusación y con una resolución judicial en forma de Auto que abre la siguiente fase, la del juicio oral. No obstante, es posible que la fase instructora, por entender el Juez de Instrucción que no existen indicios racionales de criminalidad y porque, además, nadie sostenga acusación, concluya con Auto de sobreseimiento y archivo de las actuaciones. Si por el contrario, existe dicho Auto de apertura, este delimita el hecho punible que será objeto de juicio y sentencia, y marca el inicio de la publicidad de las actuaciones, así como el final del secreto de las mismas para terceros.

En la fase de juicio oral, el procedimiento determina la existencia o no de un ilícito penal, atribuye la responsabilidad criminal del ilícito a una o unas personas determinadas y les impone una pena, para lo cual es necesario, en virtud del principio acusatorio[302], que se formule acusación, solicitando la apertura del juicio oral o la acusación pública (Ministerio Fiscal) o la acusación particular (el perjudicado o también la acusación popular).

---

[301] RODRÍGUEZ FERNÁNDEZ, R., *Prueba preconstituida y prueba anticipada. Análisis jurisprudencial,* Diario La Ley, núm. 8487, Sección Doctrina, Ref. D-68, La Ley Penal, Editorial LA LEY, 24 de febrero de 2015.

[302] FERRAJOLI, L., "Derecho y razón. Teoría del garantismo penal", 6ª edición, Editorial Trotta, Madrid, 2004, p. 93.

Más concretamente, una vez dictado el Auto de apertura del juicio oral, se dará traslado de todo lo actuado y del escrito o de los escritos de acusación a la/s defensa/s para que, a su vez, formule/n el/los escrito/s de defensa en que se rebatirán los hechos, la calificación jurídica, la autoría, o en su caso la concurrencia de circunstancias modificativas de la responsabilidad criminal, la pena y la responsabilidad civil; también se podrán proponer los medios de prueba que se estimen necesarios para practicarlos en el juicio oral.

En el procedimiento penal, solo tiene la consideración de prueba la practicada en el juicio oral, única fase en la que se garantiza la contradicción e inmediación, además de la oralidad y la publicidad[303]. La prueba es la figura más importante del proceso penal, puesto que su fin es formar la convicción del órgano judicial sobre la responsabilidad penal del acusado.

Que los únicos medios de prueba válidos para desvirtuar la presunción de inocencia sean los utilizados en el juicio oral (celebrado en condiciones de igualdad entre acusador y acusado, y con respeto a los principios de inmediación, contradicción, oralidad y publicidad), no significa que se tenga que negar toda eficacia probatoria a las diligencias de investigación en la fase de instrucción; así, por ejemplo, el atestado puede incorporar *datos objetivos y verificables, como croquis, planos,*

[303] RIFÁ SOLER, J. M., *Actos de investigación, actos de instrucción y actos de prueba*, en "Estudios sobre la prueba penal. Volumen I. Actos de investigación y medios de prueba en el proceso penal: competencia, objeto y límites", 1ª edición, Editorial LA LEY, Madrid, junio 2010.

fotografías, que pueden ser utilizados como elementos de juicio siempre que, concurriendo el doble requisito de la mera constatación de datos objetivos y de imposible reproducción en el acto del juicio oral, se introduzcan en éste como prueba documental y garantizando de forma efectiva su contradicción[304].

Como regla general, para que una diligencia de investigación pueda constituir la base probatoria sobre la que el Tribunal pueda formar su convicción, es imprescindible que sea reproducida en el acto del juicio oral para que permita la defensa del acusado, sometiéndola a contradicción y publicidad[305].

Más concretamente, existen diligencias objetivas de valor incontestable, por ejemplo, la aprehensión de los delincuentes en el lugar del delito, la ocupación o recuperación de efectos e instrumentos del delito, los croquis o fotografías obtenidas en el lugar del delito; todas ellas tienen la consideración de pruebas sometidas a la valoración del Juez o Tribunal sentenciador[306]. Los requisitos que han de reunir estos actos de

[304] Sentencias del Tribunal Constitucional 107/1983, de 29 de noviembre, FJ 3; 303/1993, de 25 de octubre, FJ 2 b); 173/1997, de 14 de octubre, FJ 2 b); 33/2000, FJ 5; 188/2002, FJ 2), citadas por la Sentencia del Tribunal Supremo, Sala Segunda, de 220/2013, de 21 de marzo.

[305] *"Cuando la diligencia sumarial es reproducida en el acto de juicio oral, adquiere carácter probatorio, aunque su resultado sea distinto"* (Sentencia del Tribunal Constitucional 98/1990, de 20 de junio).

[306] *"Así, en el transcurso de una inspección ocular en el lugar de los hechos (un robo con fuerza en un domicilio, por ejemplo), pueden recogerse huellas digitales que permitirán un cotejo posterior con los sospechosos mediante su contraste con los datos contenidos en las bases policiales. Un fluido o resto corporal del sospechoso, como la saliva o el pelo, permitirán un análisis de DNA de gran valor identificativo. Podrá analizarse la voz del sospechoso, tomarse audio, video o imagen de sus movimientos, analizarse el contenido de sus comunicaciones y los datos de tráfico y localización, estudiarse sus interacciones en el sistema económico-financiero o social, reconstruirse sus movimientos físicos, etc.".*

instrucción constitutivos de prueba sumarial preconstituida[307] para concederles valor probatorio[308] son los siguientes:

- Que se trate de diligencias de investigación de imposible o muy difícil reproducción en el juicio oral[309] debido a la fugacidad del objeto sobre el que recaen[310].

- Que sean intervenidas por el Juez de Instrucción, sin perjuicio de que también la policía judicial pueda efectuar determinadas diligencias por especiales razones de urgencia[311].

- Que se garantice la contradicción[312], permitiendo a la defensa comparecer en la ejecución de la prueba[313].

Vid., VALLÉS CAUSADA, L. M., "La policía judicial en la obtención de inteligencia…", *op. cit.,* p. 76.

[307] La expresión *prueba preconstituida* se debe a BENTHAM, derivada de la distinción que realiza entre los escritos causales y los escritos pre-constituidos, usada en su obra "Tratado de las pruebas judiciales", Capítulo VI, Libro I. Traducción por OSORIO FLORIT, Ediciones E.J.E.A., Buenos Aires, 1959.

[308] Sentencias del Tribunal Constitucional 200/1996, de 3 de diciembre, 40/1997, de 27 de febrero y 153/1997, de 29 de septiembre, y sentencias del Tribunal Supremo; Sala Segunda, de 6 de octubre de 1997, de 17 de diciembre de 1997, y de 30 de mayo de 1997.

[309] Articulo 730 de la Ley de Enjuiciamiento Criminal: *"Podrán también leerse a instancia de cualquiera de las partes las diligencias practicadas en el sumario, que, por causas independientes de la voluntad de aquéllas, no puedan ser reproducidas en el juicio oral".*

[310] Sentencias del Tribunal Constitucional 137/1988, de 7 de julio, 154/1990, de 15 de octubre, 41/1991, de 25 de febrero, 303/1993, de 25 de octubre, 323/1993, de 8 de noviembre, 79/1994, de 14 de marzo, y 51/1995, de 23 de febrero.

[311] Sentencias del Tribunal Constitucional 303/1992, de 25 de octubre, 107/1983, de 29 de noviembre, 201/1989, de 30 de noviembre, 138/1992, de 13 de octubre, y 303/1993, de 25 de octubre.

[312] Artículos 448 y 449 de la Ley de Enjuiciamiento Criminal sobre declaración de testigos; artículos 467, párrafo segundo, 471 y 476 sobre informes periciales o artículo 333 sobre inspección ocular.

[313] Sentencia del Tribunal Constitucional 303/1993, de 25 de octubre.

- Que sean introducidos en el juicio oral mediante la lectura de documentos, si bien cabría cualquier otro medio siempre que posibilitase someter su contenido a confrontación con las demás declaraciones de los intervinientes en el juicio oral[314], por ejemplo a través de preguntas formuladas en el plenario.

El no reconocer valor probatorio alguno a dichas diligencias practicadas con las debidas garantías supone para el Tribunal Constitucional[315], *"hacer depender el ejercicio del ius puniendi del Estado del azar o de la Malquerencia de las partes, pudiendo dejarse sin efecto lo actuado sumarialmente. Un sistema que pondere adecuadamente tanto la necesidad social de protección de bienes jurídicos esenciales, como el haz de garantías frente a posibles abusos de los ciudadanos, con independencia de su posición, ha de estar en condiciones de hacer valer la seriedad de lo actuado por los órganos encargados de la represión penal; siempre que lo actuado lo haya sido con pleno respeto a aquellas garantías"*.

Por tanto, son excepciones al principio general de práctica de prueba en el plenario:

[314] Sentencias del Tribunal Constitucional 25/1988, de 23 de febrero, 60/1988, de 8 de abril, 51/1990, de 26 de marzo, 140/1991, de 20 de junio y 200/1996, de 3 de diciembre.

"Cuando la diligencia sumarial es reproducida en el acto de juicio oral, adquiere carácter probatorio, aunque su resultado sea distinto" (Sentencia del Tribunal Constitucional 98/1990, de 20 de junio).

[315] Sentencias del Tribunal Constitucional 323/1993, de 8 de noviembre, que a su vez recuerda las 107/1985, de 7 de octubre, 181/1989, de 3 de noviembre y 41/1991, de 25 de febrero.

- Las diligencias sumariales, practicadas con las formalidades legales, que tengan entrada en el plenario en condiciones que permitan a la defensa del acusado someterlas a contradicción, bien como prueba documental o bien, incluso a través del contenido de las preguntas o repreguntas formuladas en el juicio[316].

- Las diligencias policiales practicadas con todas las garantías, cuyo contenido sean datos objetivos de cargo, mientras que nada revele su irrealidad[317].

- Informes y análisis periciales practicados por funcionarios adscritos a organismos oficiales, especialmente cualificados para los exámenes y trabajos que comporta la pericia que se les encomienda, si no son sometidos a juicio contradictorio por las partes, mediante la expresa impugnación del dictamen en los escritos de conclusiones, en cuyo caso han de ser sometidos a contradicción en el juicio oral como requisito de eficacia probatoria[318].

[316] Sentencia del Tribunal Supremo, Sala Segunda, 5884/1997, de 6 de octubre.

[317] Sentencias del Tribunal Supremo, Sala Segunda, de 298/1987, de 23 de enero, 2271/1987, de 31 de marzo, 2852/1987, de 22 de abril, 2867/1987, de 23 de abril, 982/1988, de 16 de febrero, 3710/1988, de 17 de mayo, 6447/1988, de 23 de septiembre y 7691/1988, de 3 de noviembre.

[318] Sentencias del Tribunal Supremo, Sala Segunda, 12627/1989, de 5 de junio, 10348/1993, de 26 de febrero, 4234/1993, de 18 de junio, 7682/1993, de 15 de noviembre, 5675/1994, de 22 de julio, 753/1994, de 11 de febrero y 1161/1994, de 23 de febrero.

- Las tasaciones periciales sobre el valor de los objetos sustraídos[319], pudiendo estas ser consideradas documentales mientras no sean impugnadas por las partes.

II.- DILIGENCIA DE OBTENCIÓN DE DATOS DE GEOLOCALIZACIÓN, COMO FUENTE DE PRUEBA Y SU INCORPORACIÓN A LA INSTRUCCIÓN

Las fuentes de prueba son elementos de la realidad, figuras extrajurídicas, que nos muestran una realidad anterior y extraña al proceso jurídico. Por el contrario, los medios de prueba son conceptos jurídicos, son las actividades que es preciso desplegar para incorporar las fuentes al proceso y que se forman durante el mismo[320]. Se buscan las fuentes para, tras su obtención, proponer medios de prueba que nos permitan incorporarlas al proceso.

Como decía SENTÍS MELENDO[321], la fuente es lo sustancial y material; el medio, lo adjetivo y lo formal. La función averiguadora se refiere a las fuentes y trata de encontrar todas aquellas susceptibles de dar lugar a medios, los cuales producirán o determinarán esa verificación

[319] Sentencia del Tribunal Supremo, Sala Segunda, 9501/1991, de 21 de junio.

[320] MONTERO AROCA, J., "Derecho jurisdiccional II. Proceso civil", edición 16ª, Editorial Tirant lo Blanch, Valencia, 2008, p.269.

[321] SENTÍS MELENDO, S., *La prueba*, en "Los grandes temas del derecho probatorio", Ediciones Jurídicas Europa-América, Buenos Aires, 1979, p. 144.

de las afirmaciones sentadas en virtud de las fuentes con las que se cuenta[322].

La diligencia de obtención de los datos de geolocalización, como diligencia de investigación que es, cumple dos funciones básicas: por un lado desempeña una función probatoria, aunque no es en sí misma un medio de prueba, sino más bien una fuente de prueba, o más exactamente una operación técnica cuyo objeto (la ubicación de un sujeto) puede crear elementos de prueba (que puedan serlo o no dependerá del contenido y de la relevancia del dato); y de otro, cumple también una importante función investigadora en cuanto que constituye una herramienta muy útil para obtener otros elementos de prueba y para decidir sobre sucesivos actos de investigación[323].

Se podría llegar a entender incluso como una actividad de aseguramiento de fuentes de prueba en condiciones de hacer posible la

---

[322] De acuerdo con la doctrina elaborada por CARNELUTTI, a quien se debe la distinción entre fuente y medio de prueba, *"en relación inmediata con el concepto de prueba como comprobación de las afirmaciones y, por otro lado, con la distinción entre prueba directa e indirecta, se encuentra el concepto de fuente de prueba que, en antítesis con el medio de prueba, constituye una de las claves de la teoría de la prueba tal como está construida en el libro anotado".*

Vid., AUGUSTI, G., Apéndice a la obra de Carnelutti, "La prueba civile", Edizioni dell' Ateno, Roma, 1947, traducción Alcalá-Zamoran y Castillo, N., Editorial Arayu, Buenos Aires, 1955, p.239.

[323] NARVAEZ RODRÍGUEZ, A., *Escuchas telefónicas: alcance constitucional y procesal,* núm. 1, Revista del Ministerio Fiscal, Madrid, 1995, p. 118.

A estas dos funciones, aplicables también a los datos de geolocalización, se ha referido la sentencia del Tribunal Supremo, Sala Segunda, de 24 de marzo de 1999, con cita de la sentencia del Tribunal Supremo de 17 de noviembre de 1994, siguiendo entre otras, la de 11 de octubre del mismo año, cuando dice que "*la intervención telefónica puede tener una doble naturaleza en el proceso penal. Puede servir de fuente de investigación de delitos, orientando la encuesta policial, o puede ella misma utilizarse como medio de prueba, en cuyo caso ha de reunir las condiciones de certeza y credibilidad que solo queda garantizado con el respeto a las leyes procesales, siendo especialmente importante el proceso de introducción de las intervenciones en la causa penal y su conversión en prueba de cargo".*

ulterior valoración jurisdiccional de los conocimientos obtenidos por esa vía[324].

La admisibilidad constitucional de la medida de obtención de los datos de geolocalización, habida cuenta de los derechos de los investigados e inculpados a no declarar contra sí mismos (artículos 17.3 y 24.2 de la Constitución Española) y a no declararse culpables (artículo 24 de la Constitución Española), y ello ante la evidencia de que el fin principal que persigue la medida es conseguir datos que ubiquen a un sujeto en el escenario de un ilícito penal, no parece plantear objeción alguna. En una ponderación adecuada y sistemática de la Constitución Española, esto no parece infringir, rigurosamente hablando, el principio constitucionalizado por el artículo 24.2 de la Constitución Española dado que, ya sean datos de geolocalización obtenidos como datos de tráfico o se encuentren insertos en una comunicación intervenida judicialmente, los mismos encuentran su fundamento, como ya se ha visto, o en el artículo 18.4 o en el 18.3 de la Constitución Española, los cuales permiten una limitación del derecho de defensa del investigado; este hecho no supone una contradicción con el artículo 24.2 de la Constitución Española, sino un complemento del mismo, siempre y cuando se respeten en la práctica todas las garantías legales que aquellos exigen.

[324] RIVES SEVA afirma en relación con la intervención de las comunicaciones que, las particularidades que rodean dicha diligencia, con inevitable anticipación al momento del juicio oral, no permiten hablar de prueba preconstituida.

Vid., RIVES SEVA, A. P., *La intervención de las comunicaciones en el proceso penal. Análisis doctrinal, legislación y jurisprudencia.,* BOSCH, 2010, p. 115

Las disposiciones comunes aplicables a la práctica de las diligencias de investigación tecnológica se ubican en los artículos 588 *bis a* al 588 *bis k* de la Ley de Enjuiciamiento Criminal, regulándose en ellos los principios a los que debe sujetarse la adopción de la medida de investigación, su alcance, contenido mínimo de la resolución judicial autorizante, duración y control de la diligencia, entre otras.

Como hemos visto en el capítulo anterior, para acordar la medida de investigación de obtención de datos de geolocalización, se impone como regla general la concesión de autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida[325]:

- El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto, lo que supone que no podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva (a saber, la investigación prospectiva).

- El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.

[325] Artículo 588 bis a de la Ley de Enjuiciamiento Criminal.

- En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:

  a) Cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o…
  b) Cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.

- Se cumple con el requisito de la proporcionalidad cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, en su trascendencia social o en el ámbito tecnológico de producción, en la intensidad de los indicios existentes y en la relevancia del resultado perseguido con la restricción del derecho.

Estas medidas de investigación tecnológica, entre las que se encuentra la obtención de los datos de geolocalización, pueden ser acordadas por el Juez, de oficio, o a instancia del Ministerio Fiscal o de la Policía Judicial[326]. En estos dos últimos casos, la petición ha de contener:

1º 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.

2º 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.

3º 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.

4º La extensión de la medida con especificación de su contenido.

5º La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.

[326] Artículo 588 bis b de la Ley de Enjuiciamiento Criminal.

6º La forma de ejecución de la medida.

7º La duración de la medida que se solicita.

8º El sujeto obligado que llevará a cabo la medida, en caso de conocerse.

Solicitada la medida, el Juez de Instrucción autorizará o denegará, en un plazo máximo de 24 horas desde la solicitud, la medida instada, oído el Ministerio Público. Concedida, la Policía Judicial ha de informar a la autoridad judicial sobre el desarrollo y resultados de la medida.

Se exige como contenido mínimo del Auto habilitante de la intervención, de conformidad con el artículo 588 bis c y e de la Ley de Enjuiciamiento Criminal:

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, que nunca podrá exceder del tiempo imprescindible para el esclarecimiento de los hechos, y que podrá ser prorrogada mediante auto motivado, por el Juez competente, de oficio o previa petición razonada del solicitante, siempre que subsistan las causas que la motivaron.

Cabe solicitar a la autoridad judicial competente la prórroga de la intervención por el Ministerio Fiscal o por la Policía Judicial con la antelación suficiente a la expiración del plazo concedido, debiendo incluir un informe detallado del resultado de la medida, así como las razones que justifiquen la continuación de la misma. Dicha solicitud de prórroga será resuelta en el plazo de los dos días siguientes a su presentación, acordando el fin de la medida o su prórroga mediante auto motivado. En este último caso, el cómputo de la duración de la medida de intervención prorrogada se iniciará desde la fecha de expiración del plazo de la medida acordada.

En cualquier caso, transcurrido el plazo por el que resultó concedida la medida, sin haberse acordado su prórroga, o, en su caso, finalizada ésta, cesará a todos los efectos.

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.

La solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa.

Se plantea por RICHARD[327] que la norma únicamente obliga a dictar Auto judicial en el supuesto de afectación de derecho fundamental, supuesto que no se da, por ejemplo, cuando el examen por la Policía Judicial de dispositivos electrónicos sea tras la cesión de los mismos por

[327] RICHARD GONZÁLEZ, M., *Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización,* Diario La Ley, núm. 8808, Sección Tribuna, Ref. D-292, Editorial LA LEY, 21 julio 2016.

particulares o empresas con el objeto de que puedan ser objeto de investigación en orden al esclarecimiento de un delito.

Lógicamente, nos mostramos conformes con este planteamiento, dado que la autorización judicial es necesaria para la injerencia de un derecho fundamental, pero no para el caso de que voluntariamente, el titular de dicho derecho, permita la afectación del mismo. Si el ciudadano, con conciencia y voluntad, permite que la Policía Judicial utilice, para el control de sus movimientos, un dispositivo de seguimiento, ello no tiene por que ser autorizado judicialmente. Otra cosa serían las posibles incidencias que de ello pudieran derivarse desde el punto de vista de la impugnación de la prueba, si el resultado de la investigación es aportado a la instrucción, toda vez que estaríamos ante un medio de prueba, en su caso, carente por ejemplo de todo control judicial durante su ejecución.

Aparece, por primera vez, regulada la posible afectación de terceras personas por las medidas de investigación acordadas[328], remitiéndose a las normas específicas que, a este respecto, existan en cada una de las medidas previstas por la Ley de Enjuiciamiento Criminal. Estamos hablando de una previsión legal dedicada a los terceros extraños y ajenos a la investigación, personas con las cuales el investigado puede comunicarse, por ejemplo, y que, sin ser sospechosas en un inicio, pueden

[328] Artículo 588 bis k de la Ley de Enjuiciamiento Criminal.

llegar a adquirir la condición también de investigadas, a resultas de la medida de investigación practicada.

Por fin, se prevé expresamente la utilización de la información obtenida en un procedimiento distinto, así como los supuestos de los descubrimientos casuales, remitiéndose a lo dispuesto en el artículo 579 bis de la Ley de Enjuiciamiento Criminal. De esta forma, se exige, para su uso, que se proceda a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia, incluyéndose entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen.

Para la continuación de la medida, en la investigación del delito casualmente descubierto, se requiere de la autorización del Juez competente, el cual comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce.

El tratamiento procesal de los hallazgos casuales, en materia de intervención de las comunicaciones, es primordial, ya que, es habitual

que a partir de la investigación de un delito, objeto de la intervención inicial, se hallen nuevos indicios de comisión de otros delitos relacionados o no, con el primero. La regulación con la que contamos en la actualidad refleja parcialmente la doctrina jurisprudencial del Tribunal Supremo, en relación con la materia.

La solución jurídica relativa a estos descubrimientos ocasionales no es uniforme en la doctrina, como expone la sentencia del Tribunal Supremo, Sala Segunda, Sección 1, 426/2016 de 19 de mayo. Hay que distinguir entre dos planteamientos[329]:

1) Si los hechos descubiertos tienen conexión[330] con los que son objeto del procedimiento de instrucción, los hallazgos surtirán efectos tanto de investigación cuanto, posteriormente, de prueba.

2) Si los hechos, ocasionalmente conocidos, no guardasen esa conexión con los causantes del acuerdo de la medida y aparentan una gravedad penal suficiente como para tolerar proporcionalmente

[329] Sentencia del Tribunal Supremo, Sala Segunda, 25/2008 de 29 de agosto.

[330] Artículo 17.2 de la Ley de Enjuiciamiento Criminal: *"2. A los efectos de la atribución de jurisdicción y de la distribución de la competencia se consideran delitos conexos:*

1º Los cometidos por dos o más personas reunidas.

2º Los cometidos por dos o más personas en distintos lugares o tiempos si hubiera precedido concierto para ello.

3º Los cometidos como medio para perpetrar otros o facilitar su ejecución.

4º Los cometidos para procurar la impunidad de otros delitos.

5º Los delitos de favorecimiento real y personal y el blanqueo de capitales respecto al delito antecedente.

6º Los cometidos por diversas personas cuando se ocasionen lesiones o daños recíprocos."

su adopción, se estimarán como mera *notitia criminis*[331] y se deducirá testimonio para que, siguiendo las normas de competencia territorial y, en su caso, las de reparto, se inicie el correspondiente proceso.

En cualquier caso, la ampliación del objeto de la investigación, a resultas de hechos descubiertos casualmente, no supone una vulneración del principio de especialidad exigido, puesto que estaríamos ante una adición o suma y no ante una novación de tipo penal investigado[332].

Una vez que se ponga término al procedimiento penal mediante resolución firme, la autoridad judicial ordenará a la Policía Judicial el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida, conservándose una copia, bajo custodia del Letrado de la Administración de Justicia.

Asimismo se acordará la destrucción, por la Policía Judicial, de las copias conservadas, incluida la custodiada por el Letrado de la

[331] Sentencias del Tribunal Supremo, Sala Segunda, 6013/1996, de 31 de octubre, 3672/1997, 26 de mayo, 196/1998, 19 de enero y 6951/1998, 23 de noviembre. En este sentido la sentencia del Tribunal Supremo, Sala Segunda, 792/2007 de 30 de mayo, recuerda que como señaló la sentencia 276/96, de 2 de abril, en estos supuestos en que se investiga un delito concreto y se descubre otro distinto, no puede renunciarse a investigar la *notitia criminis* incidentalmente descubierta en una intervención dirigida a otro fin, aunque ello pueda hacer precisa una nueva o específica autorización judicial o una investigación diferente de la del punto de arranque.

[332] Sentencias del Tribunal Supremo, Sala Segunda, 4895/1993, de 2 de julio y 135/1994, de 21 de enero.

Administración de Justicia (Secretario Judicial), cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o, cuando el delito o la pena hayan prescrito, o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal[333].

II.1.- Particularidades derivadas del modo de obtención de los datos de localización

II.1.A.- Datos de geolocalización como datos de tráfico

a) Datos de localización como datos de tráfico de valor añadido a una comunicación intervenida, no incluidos en el contenido propio de la comunicación

Cuando la medida practicada para su obtención haya sido la intervención de los datos de geolocalización, fuera del contenido propio de la comunicación y con la consideración de datos de tráfico, de conformidad con el artículo 588 ter d de la Ley de Enjuiciamiento Criminal, la solicitud de autorización judicial deberá contener, además de los requisitos generales mencionados anteriormente, la identificación del número de abonado, del terminal o de la etiqueta técnica, la conexión, objeto de intervención, o aquellos datos que sean necesarios para

[333] Artículo 588 bis k de la Ley de Enjuiciamiento Criminal.

identificar el medio de telecomunicación de que se trate, debiendo especificarse, como objeto de la solicitud, la obtención de los datos de localización geográfica del origen o destino de la comunicación.

En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al Juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El Juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.

La duración máxima inicial de la intervención, a contar desde la fecha de autorización judicial, será de tres meses, prorrogables por periodos sucesivos de duración, hasta el máximo de dieciocho meses.

Los soportes digitales, que deberán ser entregados al Juez, en aplicación del artículo 588 ter f LECrim., serán aquellos en que han quedado registrados por la policía judicial o por los intermediarios técnicos, los datos objeto de la restricción, lo cual provoca, no en pocas

ocasiones tanto dificultades técnicas en la recepción de los soportes debido a la necesidad de traducir códigos electrónicos o telemáticos a lenguaje comprensible, como complicaciones para su almacenamiento, al contar con un enorme volumen.

Otro problema que nos surge en la práctica es cómo aplicar a dichos soportes informáticos resultantes, los conceptos tradicionales de "original" y "copia". Pacífico es en la doctrina, el pensamiento de que no son aplicable a los soportes digitales los anteriormente dichos conceptos tradicionales, ya que no resulta posible establecer diferencias entre el primer soporte en el que consta la información y aquellos, que con igual formato, reproducen su contenido[334]. Es más, aunque se sostenga que siempre existirá un primer documento (*máster)*, comprobable por la fecha, a partir del cual se producirán copias, lo cierto es que (dado que la fijación de los datos en un soporte se efectúa a partir de la memoria RAM y en ésta, a su vez, a partir de su obtención a través de un instrumento de captación de información, como un escáner) el registro final es una copia, de modo que "*la propia mecánica de elaboración de un documento electrónico, cualquiera que sea, convierte el resultado en una mera copia"*[335].

[334] SANCHÍS CRESPO, C., "La prueba por soportes informáticos", Editorial Tirant lo Blanch, Valencia 1999, p. 167 y SANCHÍS CRESPO, C. y CHAVELI DONET, E. A., "La prueba por medios audiovisuales e instrumentos de archivo en la LEC 1/2000 (Doctrina, jurisprudencia y formularios)", Editorial Tirant lo Blanch, Valencia, 2002, p.122.

[335] CABEZUDO RODRÍGUEZ, N., *La Administración de Justicia ante las nuevas tecnologías. Del entusiasmo a la desconfianza, pasando por el olvido,* Revista Jurídica de Castilla y León núm.7, Administración Pública de Castilla y León, octubre 2005, p.155-208.

De esta forma, en el caso de los datos de geolocalización como datos de tráfico, el soporte "original" ha de ser el sistema de archivo informático o electrónico en el que se almacene la información[336]. En cualquier caso, deberá asegurarse la autenticidad y la integridad de dicha información volcada sobre datos de geolocalización desde el ordenador central a los soportes digitales, mediante un sistema de sellado de firma electrónica avanzado o sistema de adveración suficientemente fiable[337].

GONZÁLEZ LÓPEZ[338] aporta como solución a diversos problemas en relación con los datos de tráfico, y más concretamente en relación con la posible impugnación del contenido del archivo que contiene la información, la conveniencia de copiar la totalidad del archivo con adveración del Letrado de la Administración de Justicia, hecho que, a nuestro juicio, no sería nada positivo ya que este funcionario es fedatario público y no técnico informático, de modo que pocas garantías puede aportar al proceso al no ostentar la cualificación técnica adecuada, añadiéndose que sería además tarea imposible en un Juzgado de Instrucción, con un volumen considerable de causas (algo que ocurre en prácticamente todos los órganos judiciales españoles) ya que se

Otros autores como DE URBANO CASTRILLO sí defienden la existencia de un documento original, aunque a falta de legislación específica sobre la materia que permita establecer cuándo se está en presencia del original y cuando de una copia, entiende que será necesaria la prueba pericial.

Vid., DE URBANO CASTRILLO, E., *El documento electrónico: aspectos procesales,* en VV.AA., "Internet y derecho penal", Consejo General del Poder Judicial, Madrid, 2001, pp. 595 y 596.

336 RODRÍGUEZ LAÍNZ, J. L., "La intervención judicial en los datos de tráfico de las comunicaciones", Editorial BOSCH, Barcelona 2003.

337 Por aplicación analógica del artículo 588 ter f LECrim. dedicado a la intervención de las comunicaciones en general.

338 GONZÁLEZ LÓPEZ, J. J., "Los datos de tráfico de las comunicaciones electrónicas en el proceso penal", Editorial LA LEY, Madrid 2007, pp. 483-486.

convertiría dicha adveración en la única misión del Letrado de la Administración de Justicia por escasez de tiempo.

Otra cuestión a debatir es si cabe la incorporación de los datos de tráfico al proceso, de manera distinta a la entrega directa de los mismos al instructor.

En la práctica diaria, y admitido por el Alto Tribunal[339], la incorporación en general de los datos de tráfico no se realiza a través de su entrega al instructor, sino que usualmente se efectúa mediante su inclusión en el atestado, para su posterior entrega en el Juzgado.

b) Datos de localización ubicados en archivos automatizados de los prestadores de servicios, sin que exista intervención de las comunicaciones

Si la obtención de los datos de localización se ha realizado fuera de una intervención de las comunicaciones, y se pretende su incorporación al proceso como datos obrantes en archivos automatizados de los prestadores de servicios, los mismos solo podrán ser cedidos mediando

[339] La sentencia del Tribunal Supremo, Sala Segunda, 1231/2003, de 25 de septiembre, admite que los listados de llamadas facilitados por la compañía telefónica, a pesar de serlo como consecuencia de una petición judicial, sean entregados a las fuerzas policiales e incorporados al atestado, lo que podría ser aplicable asimismo a los datos de geolocalización como datos de tráfico.

GONZÁLEZ LÓPEZ critica lo anterior, puesto que estima que la admisión de esta conducta implicaría rebajar la importancia de este tipo de injerencias y tolerar respecto de la policía, lo que se niega al Ministerio Fiscal (así, el acopio directo de la información).

Vid., GONZÁLEZ LÓPEZ, J. J., "Los datos de tráfico de las comunicaciones electrónicas…", *op. cit.*, p. 487.

previa autorización judicial[340], la cual se otorgará cuando el conocimiento de dichos datos sea imprescindible para la investigación y, así, se justifique por los investigadores.

Esta exigencia de autorización judicial ya existía para la *cesión de datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación* (tráfico de llamadas, identificación del titular del teléfono, localización de terminal etc.), en aplicación del artículo 7 de la Ley 25/2007, de 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.

En este caso, en cumplimiento del deber de colaboración[341], y bajo apercibimiento de poder incurrir en delito de desobediencia en caso de incumplimiento, con obligación asimismo de guardar secreto acerca de las actividades requeridas, todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar al Juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la

[340] Artículo 588 ter j de la Ley de Enjuiciamiento Criminal.
[341] Artículo 588 ter e de la Ley de Enjuiciamiento Criminal.

medida, la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones.

Como ya se ha expuesto en el Capítulo anterior, la expresión (*"así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual")* no se puede considerar acertada debido a su falta de concreción, toda vez que estamos ante un sujeto activo, objeto del deber, presentado de manera genérica y susceptible de interpretación, lo cual sin duda genera inseguridad jurídica.

II.1.B.- Datos de geolocalización incluidos en el contenido de la comunicación intervenida judicialmente

La comunicación privada realizada mediante dispositivos de comunicación electrónicos, como teléfonos u ordenadores, puede ser objeto de investigación mediante la diligencia de intervención de las comunicaciones telefónicas y telemáticas prevista en los artículos 588 ter a-m de la Ley de Enjuiciamiento Criminal, regulación que sustituye al insuficiente artículo 579 del texto procesal.

Supone la posibilidad de intervenir comunicaciones de toda clase, así las clásicas orales, comunicaciones donde se incluyan transmisión de fotografías (hay que recordar que en ellas aparecen los archivos *Exif*, que

nos indican la ubicación geográfica donde se hizo la instantánea), mensajes de texto o comunicaciones a través de mensajería instantánea (a modo ejemplar, *WhatsApp*) donde podemos transmitir a nuestro interlocutor datos como nuestra ubicación en el espacio.

La obtención de estos datos de geolocalización provendrá, como ya se ha explicado, de la intervención de las comunicaciones mediando siempre autorización judicial, con una única excepción para el caso de urgencia[342]. En dicho supuesto, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad.

Para la legitimidad de esta medida, han de ser objeto de intervención los terminales o medios de comunicación habitual u ocasionalmente utilizados por el investigado, ya sea como emisor o como receptor de la comunicación, o incluso los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad.

La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación

[342] Artículo 588 ter d de la Ley de Enjuiciamiento Criminal.

tenga por objeto 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 (artículo 579.1 de la Ley de Enjuiciamiento Criminal) o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

Dicha autorización está sometida al cumplimiento de los principios rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida, explicados anteriormente.

La solicitud de autorización judicial de intervención[343], aparte de los requisitos comunes ya expuestos, identificará el número de abonado, del terminal o de la etiqueta técnica, la conexión objeto de intervención o aquellos datos que sean necesarios para identificar el medio de telecomunicación de que se trate.

La duración máxima inicial de la intervención, a contar desde la fecha de autorización judicial, será de tres meses, prorrogables por periodos sucesivos de duración, hasta un máximo de dieciocho meses.

A efectos de control de la medida, la Policía Judicial pondrá a disposición del Juez, con la periodicidad que este determine y en soportes digitales distintos, la transcripción de los pasajes que considere de

[343] Artículo 588 ter d de la Ley de Enjuiciamiento Criminal.

interés y las grabaciones íntegras realizadas. Se indicará el origen y destino de cada una de ellas y se asegurará, mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas.

Como novedad se regula la posibilidad de afectación a terceros, así se prevé la intervención judicial de las comunicaciones emitidas por terminales pertenecientes a terceros ajenos a la investigación, siempre que se de una de estas tres posibilidades[344]:

a) Que exista constancia de que el sujeto investigado se sirve de aquellos terminales para transmitir o recibir información.

b) Que el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad.

c) Que el dispositivo, objeto de investigación, sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular.

Alzado el secreto, acordado obligatoriamente en estas actuaciones, y terminada la vigencia de la medida de intervención, se entregará a las

[344] Artículo 588 ter c de la Ley de Enjuiciamiento Criminal.

partes copia de las grabaciones y de las transcripciones realizadas, en este caso incluyendo los datos de localización que hayan formado parte de la comunicación. Si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos, haciéndolo constar de un modo expreso[345].

Examinado lo anterior por las partes, cualquiera de ellas podrá solicitar la inclusión en las copias de aquellas comunicaciones que incluyan datos de geolocalización que entiendan relevantes y que hayan sido excluidas, decidiendo la autoridad judicial, tras oírlas, sobre la exclusión o incorporación a la causa.

En este punto, el Juez de Instrucción competente notificará a las personas intervinientes en las comunicaciones interceptadas, el hecho de la práctica de la injerencia, informándolas de las concretas comunicaciones en las que hayan participado y que resulten afectadas, salvo que sea imposible, que exija un esfuerzo desproporcionado o perjudique futuras investigaciones, pudiendo solicitar la persona notificada la entrega de copia de la grabación o la transcripción de las comunicaciones, siempre que no afecte al derecho a la intimidad de otras personas o sea contrario a los fines del proceso en cuyo marco se hubiera adoptado la medida. Entendemos que la regla general será el cumplimiento del mandato legal de comunicación a terceros y que, en

[345] Artículo 588 ter l de la Ley de Enjuiciamiento Criminal.

caso contrario, habrá de motivarse su no cumplimiento, puesto que de no ser así, podría darse la mala praxis de, justificándose en la extrema carga de trabajo de los Juzgados, mal endémico de los mismos, nunca informar a esos terceros afectados.

II.1.C.- Datos de geolocalización obtenidos mediante dispositivos técnicos de seguimiento o balizas

La Ley de Enjuiciamiento Criminal[346], tras su modificación experimentada por la LO 13/2015, regula, por primera vez, el control de los movimientos, desplazamientos y estancias, en un lugar determinado, de los ciudadanos, con el objeto de investigar la comisión de delitos. Sorprende que esta regulación específica haya olvidado determinar cuáles son los delitos que pueden ser objeto de investigación mediante el uso de estos dispositivos técnicos de seguimiento.

Para el caso de utilización de dispositivos técnicos de seguimiento y localización por los investigadores, y siempre que concurran acreditadas razones de necesidad y la medida resulte proporcional, el Juez podrá autorizar su uso y con ello obtener datos de geolocalización, siempre concretando el medio técnico que va a ser usado. Si mediaran razones de urgencia que hagan razonable temer que, de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y

[346] Artículo 588 quinquies b de la Ley de Enjuiciamiento Criminal.

localización, se frustrara la investigación, la Policía Judicial podrá proceder a su colocación dando cuenta, a la mayor brevedad posible, y máximo en 24 horas, a la autoridad judicial, quien podrá ratificar la medida adoptada o acordar su cese inmediato.

En este último supuesto, caso de que los agentes actuantes, por razones de urgencia, hubieran usado este instrumento de seguimiento sin contar con la previa autorización judicial, y si al dar cuenta al instructor éste decretase su cese, la información obtenida a partir de la baliza colocada carecerá de efectos en el proceso, es decir, carecerá de toda validez probatoria[347].

La introducción de los datos en el proceso se realizará mediante la entrega por la Policía Judicial al Juez, de los soportes originales o copias electrónicas auténticas que contengan la información recogida cuando éste se lo solicite y, en todo caso, cuando terminen las investigaciones.

Volvemos de nuevo al problema, ya mencionado, de posible identificación de un soporte donde constan datos electrónicos como

[347] RICHARD expone que no es suficiente declarar que lo obtenido no tiene efectos en el proceso, y ello por entender que el contenido de dicha norma es obvio y por tanto innecesario, añadiendo que habilita la existencia de *"seguimientos comunicados (o no comunicados) al Juez basados simplemente en la consideración policial de urgencia que puede frustrar una investigación. […]El que ha redactado la Ley ha oído las necesidades de la policía que, naturalmente, es una parte del sistema de Justicia expansivo por su propia naturaleza y no ha pensado en las consecuencias de esta normativa. Por esa razón, en orden a comenzar a implementar un control de la actividad de la policía ¿Qué tal si registramos todos los dispositivos de seguimiento y se controla su uso por la Fiscalía dando cuenta a la autoridad judicial gubernativa (Salas de gobierno, presidencia audiencia, Jueces decanos según el caso)?".*

Vid., RICHARD GONZÁLEZ, M., *Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización,* Diario La Ley, núm. 8808, Sección Tribuna, Ref. D-292, Editorial LA LEY, 21 julio 2016.

"auténtico", o como "copia". La recepción de los datos de la baliza se reciben en cualquier dispositivo que cuente con el programa adecuado, así como el nombre de usuario y contraseña exigida, al no existir un sistema parejo a SITEL que oficialice de alguna forma esta recogida de datos.

La duración máxima de la medida será de tres meses, a partir de la fecha de autorización judicial, aunque excepcionalmente el Juez puede acordar prórrogas sucesivas por el mismo o inferior plazo hasta un máximo de dieciocho meses, si estuviera justificado a la vista de los resultados ya obtenidos.

De manera muy genérica e insuficiente, se prevé que la información obtenida a través de estos dispositivos técnicos de seguimiento y localización sea debidamente custodiada para evitar su utilización indebida, pero todo esto se lleva a cabo sin determinar a quien le corresponde la custodia en cada momento, en qué consiste dicha custodia o qué se entiende por "utilización indebida".

II.1.D.- Datos de geolocalización obtenidos mediante número IP

Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en Internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo

utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del Juez de Instrucción que requiera de los agentes sujetos al deber de colaboración[348], la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso[349].

II.2.- Custodia y selección de datos relevantes

Como ya se ha avanzado, los soportes físicos que contienen la información han de quedar bajo la custodia del Letrado de la Administración de Justicia, que adoptará las medidas necesarias para garantizar su conservación, a fin de asegurar la práctica de los medios probatorios a éstos concernientes y la posibilidad de contradicción de las partes.

[348] Según el artículo 588 ter ede la Ley de Enjuiciamiento Criminal, lo son los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual.

[349] Artículo 588 ter k de la Ley de Enjuiciamiento Criminal.

Se trata de garantizar, en definitiva, la seguridad de los datos de tráfico[350] y, más concretamente, de los de geolocalización.

Se echa en falta una regulación expresa que concrete las condiciones precisas en que deben ser conservados tales datos, no solo por parte de los proveedores, sino también por el Letrado de la Administración de Justicia, ya que se requiere una atención específica que no queda resuelta por la remisión genérica a las normas de protección de datos. Tampoco existe previsión alguna al respecto en la nueva redacción de la Ley de Enjuiciamiento Criminal, tras sus últimas modificaciones de octubre de 2015, habiéndose desperdiciado, en consecuencia, la oportunidad de legislar pormenorizadamente una materia que en la práctica supone muchos quebraderos de cabeza, y que es motivo, por parte de las defensas, de constantes impugnaciones, con mayor o menor sentido.

De una forma muy genérica e insuficiente, para el caso de los datos de localización obtenidos a través de utilización de dispositivos técnicos de seguimiento, la Ley de Enjuiciamiento Criminal[351] dispone únicamente que la información obtenida deberá ser debidamente custodiada para evitar su utilización indebida; esta disposición, como ya hemos expuesto en apartado anteriores, suscita numerosas dudas. En el caso de la intervención judicial de las comunicaciones donde consten los datos de

[350] DAVARA RODRÍGUEZ, M. A., *Instrucción penal y nuevas tecnologías,* en "El Juez de instrucción y Juez de garantías: posibles alternativas", Consejo General del Poder Judicial, Madrid, 2002, p. 189.

[351] Artículo 588 quinquies c 3 de la Ley de Enjuiciamiento Criminal.

localización como datos de tráfico o dentro del contenido de la comunicación propiamente dicha, hemos de acudir a las disposiciones generales, donde tampoco se establece un procedimiento específico respecto a la custodia de los originales.

Previo a la custodia por el Letrado de la Administración de Justicia de los originales que se entreguen a la autoridad judicial en el ámbito del control de la medida, resulta de vital importancia la garantía de la "cadena de custodia", a fin de que la información no se vea alterada, porque se entiende que, en relación con los soportes digitales o electrónicos, la garantía de inalterabilidad se basa en el establecimiento de protocolos de seguridad que garanticen la integridad de la información[352].

La cadena de custodia constituye un sistema formal de garantía que tiene por finalidad dejar constancia de todas las actividades llevadas a cabo por cada una de las personas que se ponen en contacto con las evidencias[353].

Es a través de la cadena de custodia como se satisface la garantía de lo que se ha denominado la "mismidad de la prueba"[354]. A tal respecto, se ha dicho por la doctrina que la cadena de custodia es una figura tomada de la realidad a la que tiñe de valor jurídico con el fin de, en su

[352] RODRÍGUEZ LAÍNZ, J. L., "La intervención judicial en los datos de tráfico…", *op. cit.*, p. 163.
[353] Sentencia del Tribunal Supremo, Sala Segunda, 587/2014, de 18 de julio.
[354] Sentencia del Tribunal Supremo, Sala Segunda, 1190/2009, de 3 diciembre.

caso, identificar el objeto intervenido, pues al tener que pasar por distintos lugares para que se verifiquen los correspondientes exámenes, es necesario tener la seguridad de que lo que se traslada y analiza es lo mismo en todo momento, desde que se recoge en el lugar del delito, hasta el momento final que se estudia y, en su caso, se destruye[355].

De nuevo nos encontramos con una ausencia de regulación expresa en la legislación vigente tras la Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica de 2015. Como dice RUBIO[356], el sentido común, la buena fe de los funcionarios, la presunción de veracidad de éstos y la jurisprudencia, guían las actuaciones en pro de la conservación de la cadena de custodia de las pruebas.

Por último, se plantea la cuestión de cuál es el órgano competente para practicar la **selección del material** recabado que se debe incorporar al juicio oral. GONZÁLEZ LÓPEZ[357] defiende que esta selección ha de ser practicada por el Juez, y nunca por la Policía Judicial, debiéndose dejar constancia de tal proceso por el Letrado de la Administración de Justicia, como dador de fe de las actuaciones judiciales, debiendo de consistir en dos selecciones, una que tiene como finalidad excluir los

[355] Sentencia del Tribunal Supremo, Sala Segunda, 615/2014, de 25 de septiembre.

[356] RUBIO ALAMILLO, J., *Conservación de la cadena de custodia de una evidencia informática,* Diario La Ley, núm. 8859, Sección Doctrina, Ref. D-389, Editorial Wolters Kluwer, 9 noviembre 2016.

[357] GONZÁLEZ LÓPEZ, J.J., "Los datos de tráfico de las comunicaciones electrónicas…", *op. cit.*, p. 498.

datos que afecten a personas no investigadas (su realización correspondería al Juez, sin contradicción ni presencia de los afectados distintos al imputado/investigado), y otra, la que excluiría las conversaciones no vinculadas con los hechos investigados, cumpliendo con el requisito de contradicción[358].

Si atendemos al artículo 588 ter f LECrim., el cual dispone que en una intervención de las comunicaciones será la Policía Judicial quien se encargará de transcribir los pasajes que considere de interés, si bien habrá de entregar al Juez competente las grabaciones íntegras, podemos interpretar que, en la geolocalización, los datos habrán de ser también puestos a disposición de la autoridad judicial de manera íntegra, sin perjuicio del análisis de los mismos que pueda efectuar la fuerza actuante en el correspondiente atestado. De igual modo que para las comunicaciones interceptadas, se debería exigir un sistema de sellado o de firma electrónica avanzado o sistema de adveración suficientemente fiable a los efectos de garantizar la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales.

Más concretamente[359], la Policía Judicial entregará al Juez los soportes originales o copias electrónicas auténticas que contengan la información de geolocalización recogida cuando éste lo solicite, y en todo caso, cuando terminen las investigaciones.

[358] MONTERO AROCA, J., "La intervención de las comunicaciones electrónicas en el proceso penal: un estudio jurisprudencial", Editorial Tirant lo Blanch, Valencia, 1999, p. 246.

[359] Artículo 588 quinquies c de la Ley de Enjuiciamiento Criminal.

III.- DATOS DE GEOLOCALIZACIÓN COMO MEDIO DE PRUEBA

Los medios de prueba son los mecanismos legales que establece en el ordenamiento jurídico el legislador para facilitar la prueba sobre los hechos. Son las herramientas jurídicas que permiten al Tribunal llegar a obtener una convicción sobre el hecho criminal traído al proceso, en el debate contradictorio de las partes procesales sobre los elementos empíricos (LEAL MEDINA[360]).

La diferencia fundamental entre lo que han sido las diligencias de investigación durante la instrucción del procedimiento y los medios de prueba, que habrán de practicarse en el juicio oral[361], estriba en que éstos han de realizarse siempre ante órgano jurisdiccional, y con estricto respeto a los principios constitucionales de publicidad, oralidad y, especialmente contradicción entre las partes (acusación y defensa) e inmediación[362] del Tribunal sentenciador (unipersonal o colegiado)[363].

---

[360] LEAL MEDINA, J., *Ruptura de la cadena de custodia y desconexión con las fuentes de prueba. Supuestos concretos. Reflexiones que plantea.,* Diario La Ley, núm. 8846, Sección Doctrina, 19 octubre 2016, Ref. D-367, Editorial Wolters Kluwer, 19 de octubre de 2016.

[361] LÓPEZ ORTEGA, J. J., *Contradicción y defensa. Cinco cuestiones sobre la prueba penal, precedidas de una introducción sobre la eficiencia del proceso penal,* en "La generalización del Derecho Penal de excepción: tendencias legislativas", Estudios de Derecho Judicial 128/2007, Consejo General del Poder Judicial, Madrid, 2007, p. 13.

[362] Sentencia del Tribunal Supremo, Sala Segunda, 7285/1995, de 4 de mayo: *"... las diligencias probatorias sometidas a la íntima convicción del Tribunal han de propiciarse:*

Integrados ya los datos de geolocalización en el proceso penal, nos planteamos cómo impugnarlos, qué valor probatorio ostentan y las consecuencias de una hipotética declaración de ilicitud, como prueba.

III.1.- La impugnación del medio de prueba

Pese a los recelos que por novedosos suscitan los soportes informáticos, éstos, por sí solos, son prueba bastante para fundamentar la convicción judicial.

Como sustento de la anterior afirmación, podemos traer a colación las soluciones jurisprudenciales proporcionadas en relación con las grabaciones videográficas y las cintas resultantes de la intervención de las comunicaciones.

Así, a este respecto, se sostiene que solo cuando se impugne su autenticidad será necesario acudir a medios de prueba auxiliares, siendo la parte impugnante quien ha de solicitar la prueba pericial

a) con publicidad y oralidad para que sin secretismo alguno pueda conocerse el desarrollo de la función jurisdiccional por todos los miembros de la sociedad.

b) con inmediación para que ese ejercicio jurisdiccional tenga lugar ante quienes van a percibir por sus sentidos lo que ya después otros ojos y oídos no van a ver ni oír.

c) con contradicción de parte para facilitar a los intervinientes la defensa de sus respectivas pretensiones, defendiendo sus pruebas y refutando las ajenas."

[363] RODRÍGUEZ FERNÁNDEZ, R., *Prueba preconstituida y prueba anticipada…, op. cit.*

correspondiente[364]. Por tanto, aportado el medio de prueba por la acusación, recae sobre la parte contraria la carga de devaluar o eliminar la fuerza probatoria de los soportes presentados, debiendo no solo impugnarlos, sino también proponer los medios de prueba orientados a acreditar la falta de autenticidad de tales soportes.

No nos mostramos conformes con la crítica que, a este respecto, realizan tanto GONZÁLEZ LÓPEZ[365] como RODRÍGUEZ LAINZ[366], quienes defienden que en cualquier caso, tras la impugnación, los medios de prueba auxiliares habrán de ser propuestos por la acusación, por entender que ello conllevaría como resultado continuas impugnaciones sin fundamento, con la dilación del procedimiento que supondría la práctica de nueva prueba que corrobore a la impugnada. En todo caso, habría de ser la parte impugnante la que motive su posición y ofrezca medios de prueba auxiliares, abriendo así, si está fundamentado, el debate con la parte acusadora que entonces sí, deberá proponer los suyos para contrarrestar esa impugnación.

En cuanto a la prueba auxiliar, o prueba pericial que ha de corroborar el soporte informático, su valoración, como no debe de ser de otro modo, corresponderá al Juez, sin perjuicio de que, por la

[364] Sentencia del Tribunal Supremo, Sala Segunda, 1075/2004, de 24 de septiembre, FJ1, 705/2005, de 6 de junio, FJ7, y 1566/2005, de 30 de diciembre, FJ1.

[365] GONZÁLEZ LÓPEZ, J. J., "Los datos de tráfico de las comunicaciones electrónicas…", *op. cit.*, p. 520.

[366] RODRÍGUEZ LAINZ, J. L., "La intervención judicial en los datos de tráfico…", *op. cit.*, p. 378.

complejidad de la materia en la mayoría de las ocasiones, la decisión judicial quede sujeta a la opinión del perito experto[367].

En el caso concreto de los datos de tráfico, ciertamente la manipulación de los mismos, no se encuentra al alcance del público en general, por lo que se ha estimado que una adecuada conformación por el operador de comunicaciones y recepción en el proceso aseguran un alto grado de fiabilidad[368].

Es preciso cuestionarse si, al igual que sucede con los documentos cuyo soporte es el papel, resulta posible poner en duda la autenticidad de los soportes informáticos (quedan fuera aquellos datos de localización como datos de tráfico obtenidos a través de interceptación de las comunicaciones mediante el sistema SITEL, del que hablaremos posteriormente).

Para GONZÁLEZ LÓPEZ sería imposible referirse a la falta de autenticidad de los soportes que contienen los datos de tráfico, dado que dichos soportes corresponden a la categoría de "documento

[367] ROMEO CASABONA sostiene que "*no es posible imaginar que ante conclusiones técnicas, artísticas o científicas emitidas por expertos (a veces muy cualificados) el juez por su propia autoridad disienta y siga conclusiones contrarias, ya que ello puede resultar no solo escandaloso sino incluso sospechoso en orden a la imparcialidad que debe rodear siempre al juez*".

Vid., ROMEO CASABONA, C. M., *Los perfiles de ADN en el proceso penal: novedades y carencias del Derecho español,* en "Las reformas procesales", Consejo General del Poder Judicial, Madrid 2005, p. 425.

[368] RODRÍGUEZ LAÍNZ, J. L., "Juzgado de Violencia sobre la Mujer y Juzgado de Guardia", Editorial BOSCH, Barcelona 2006, p. 213.

representativo", frente a la de "documento declarativo"[369], es decir que los soportes que contienen los datos de tráfico referidos a unas determinadas comunicaciones no reflejan declaraciones, sino estado de cosas, de modo que para que el contenido no se corresponda con la realidad sería necesario modificar el soporte.

Difícil se antoja la impugnación del contenido de los archivos automatizados de los prestadores de servicios, debido a su propia naturaleza, y más si a ello añadimos el necesario establecimiento de protocolos de seguridad que garanticen la integridad de la información, como así se prevé en la nueva redacción de la Ley de Enjuiciamiento Criminal, conforme se ha visto en apartados anteriores.

Respecto a la obtención de los datos de geolocalización obtenidos a través de una intervención judicial de la comunicaciones, ya sea en su condición de datos de tráfico o en la de contenido propio de la comunicación, se parte, como ha sido expuesto por la doctrina constitucional[370], de que una injerencia puede constituir una vulneración del derecho al secreto de las comunicaciones si no se respetan las garantías constitucionales a él inherentes en alguna de las fases diferenciables en el curso del proceso: en primer lugar, en la decisión de

[369] GONZÁLEZ LÓPEZ, J. J., "Los datos de tráfico de las comunicaciones electrónicas…", *op.cit.*, p.501, recuerda a MOLINS GARCIA-ATANCE, J., *Impugnación y autenticidad documental,* Diario La Ley, núm. 6143, Editorial LA LEY, diciembre 2004.

[370] Sentencia del Tribunal Constitucional 121/1998, de 15 de junio, FJ 5º, ratificado en la 151/1998, de 13 de julio FJ4, y recordada ambas en la sentencia del Tribunal Constitucional 166/1999, de 27 de septiembre.

intervención, en segundo lugar, en su ejecución policial, y en tercer lugar, en el control judicial de la ejecución.

a) La decisión de intervención no es legítima:

- Si no ha sido adoptada por un órgano judicial[371].
- Si se da la carencia de presupuestos materiales que habilitan legal y constitucionalmente la adopción de la decisión judicial de intervención, cuya ausencia convierte a la medida en desproporcionada.
- Si la medida no es de estricta necesidad; es decir, puede ser constitucionalmente ilegítima, dado su carácter prescindible, bien porque los conocimientos que pueden ser obtenidos carecen de relevancia respecto de la investigación del hecho delictivo o respecto de la conexión de las personas investigadas, o bien porque pudieran obtenerse a través de otras medidas menos gravosas de los derechos fundamentales en litigio[372].
- Si falta expresión o exteriorización, tanto de la existencia de los presupuestos materiales de la intervención -investigación, delito grave, conexión de las personas con los hechos- como de la necesidad y adecuación de la medida, razones y finalidad

[371] Sentencia del Tribunal Constitucional 86/1995 de 6 de junio, FJ3: *"[…] es evidente que la escucha telefónica practicada sin autorización judicial constituye una violación flagrante del derecho al secreto de las comunicaciones".*

[372] Sentencias del Tribunal Constitucional 54/1996, de 26 de marzo, FJ 8 y 49/1999, de 5 de abril FFJJ 7 y 8.

perseguida[373], siendo todo ello también exigible, respecto de las decisiones de mantenimiento de la medida, en cuyo caso, además, deben ponderarse las concretas circunstancias concurrentes en cada momento y el conocimiento adquirido a través de la ejecución de la medida inicialmente prevista[374].

b) La ejecución policial es ilegítima si se verifica excediéndose de la cobertura judicial, o dicho de otro modo, excediéndose de los límites temporales (manteniéndose la intervención más tiempo del habilitado), de los personales (por ejemplo, si se investigan personas distintas de las autorizadas), o de los materiales (hechos diferentes), u otros límites que constituyan condiciones judicialmente impuestas de la autorización y que no se respeten[375].

c) La ilegitimidad podría proceder de la deficiencia o ausencia del control judicial. Por ejemplo, el caso de falta de fijación judicial de los períodos en los que debe darse cuenta al Juez de los resultados de la restricción; igualmente si el Juez no efectúa un seguimiento de las vicisitudes del desarrollo y cese de la intervención telefónica, y si no conoce el resultado obtenido en la investigación[376].

---

[373] Sentencia del Tribunal Constitucional 54/1996, de 26 de marzo, FJ8.

[374] Sentencia del Tribunal Constitucional 49/1999, de 5 de abril, FJ 11.

[375] Sentencias del Tribunal Constitucional 85/1994, de 14 de marzo FJ 3, 86/1995, de 6 de junio, FJ 3, 49/1996, de 26 de marzo FJ 3 y 121/1998, de 15 de junio FJ 5.

[376] Sentencia del Tribunal Constitucional 49/1999 de 5 de abril, FJ 5.

La falta de los datos indispensables en el oficio policial (investigación previa realizada, resultado provisional, concreción del delito que se investiga, personas a investigar, teléfonos a intervenir y el plazo de intervención) no puede ser justificada a posteriori por el éxito de la investigación misma (sentencias del Tribunal Constitucional

En resumen, hay que tener por infracciones de alcance constitucional en la materia, la ausencia de fundamento bastante de la autorización, la conculcación del principio de proporcionalidad que ha de regir la decisión del Juez, por supuesto la absoluta ausencia del acuerdo judicial o los defectos trascendentales en el mismo, como la total omisión de motivación y la absoluta indeterminación de la clase de delito perseguido, de la identificación del sujeto pasivo o de los encargados de ejecutar la diligencia, de los números telefónicos a intervenir o de los límites temporales para la ejecución de la restricción del derecho fundamental y periodicidad de entrega de los informes al Juzgado, por parte de los ejecutores de la práctica. También tendrán el mismo carácter las graves incorrecciones en la ejecución de lo acordado, que supongan una extralimitación en el quebranto de los derechos del afectado o de terceros, prórrogas temporales o extensiones a otros teléfonos no autorizados expresamente y, en definitiva, cualquier actuación de los investigadores que incumpla lo dispuesto por el Instructor en lo relativo a los límites constitucionalmente protegidos[377].

La sentencia del Tribunal Supremo, Sala Segunda, de 12 de diciembre de 1994 declara que "*la absoluta falta de motivación de la resolución judicial habilitante de la invasión del espacio protegido de la intimidad personal supone una vulneración del derecho constitucional al secreto de las comunicaciones telefónicas proclamado en el artículo 18.3 de*

253/2006, de 11 de septiembre; 165/2005, de 20 de junio; 259/2005, de 24 de octubre).

[377] Sentencia del Tribunal Supremo, Sala Segunda, 343/2007, de 20 de abril, FJ4.

la Constitución Española" y recuerda que el Tribunal Constitucional en su sentencia de 14 de marzo de 1994, y una reiterada doctrina de esta Sala, han mantenido que la falta de motivación de la resolución judicial que autorizó la escucha contradice el derecho a la tutela judicial efectiva y supone la nulidad de su resultado y de todas las actuaciones que traigan su causa del contenido de las grabaciones.

La inexistencia de indicios en que fundamentar el Auto acordando la medida, que por tanto resultaría caprichoso o arbitrario, vulneraría según LÓPEZ-BARJA[378] el derecho a la tutela judicial efectiva que los Jueces y Tribunales deben otorgar en aplicación del artículo 24.1 de la Constitución Española.

En la misma línea, FERNÁNDEZ-ESPINAR[379] piensa que *"la sospecha fundamentada de la injerencia en este derecho fundamental debe revestir intensidad y reclamarse exquisitamente del material fáctico preexistente en la causa, debiendo albergarse la duda en el ánimo del Juez y siendo, por todo lo dicho, inviable que una escucha ocasione la formación de una causa, dado que el proceder es inverso, es decir, se ordena una intervención telefónica en mérito a la posibilidad racional –con los datos que operan en el poder del Juez- de obtener el descubrimiento o comprobación de algún hecho relevante para la causa"*. Así señalan la

[378] LÓPEZ-BARJA DE QUIROGA, J., "Las escuchas telefónicas y la prueba ilegalmente obtenida", Editorial Akal, Madrid, 1989.

[379] FERNÁNDEZ-ESPINAR, G., *El levantamiento del secreto de las comunicaciones telefónicas en el marco de las diligencias de investigación y aseguramiento en el proceso penal,* Poder Judicial, núm. 32, Consejo General del Poder Judicial, Madrid, diciembre de 1993, p. 28.

consecuencia anulatoria de la intervención telefónica por basarse en meras sospechas e indicios insuficientes, a modo ejemplar, las sentencias del Tribunal Supremo, Sala Segunda, de 15 de diciembre de 2003[380], 15 de febrero de 2003, 24 de abril de 2003, 6 de octubre de 2004, 28 de marzo de 2005 y 16 de octubre de 2006.

Asimismo, se producirá una vulneración del derecho desde el momento en que expira la orden judicial sin ser renovada[381]. Los efectos de la extralimitación en el plazo sería la nulidad de las escuchas efectuadas en días sin cobertura judicial y, por ello mismo, las conversaciones grabadas durante esos días no pueden desplegar efectos probatorios (sentencia del Tribunal Constitucional 26/2006, de 30 de enero y 205/2005, de 18 de julio).

[380] La sentencia del Tribunal Supremo, Sala Segunda, 1690/2003, de 15 de diciembre contempló el siguiente supuesto: *"El Comisario Jefe de Albacete formuló solicitud de interceptación de los teléfonos móviles del recurrente sobre la base de las siguientes afirmaciones: a) que realiza viajes a Madrid y Alicante para adquirir cocaína y hachís; b) que viaja en un vehículo Volkswagen Golf, de matrícula 8434-BJJ, acompañado de un individuo de raza árabe, Ernesto, que le sirve de contacto y luego trabaja como camello; c) que el nombre de este individuo figuraba en una documentación intervenida a algunos sujetos relacionados con el tráfico de drogas; d) que Emilio, cuando llega a Albacete con ese turismo se introduce en una cochera, donde tiene también una furgoneta; e) que cuando se desplaza a Madrid lo hace con su mujer e hijos para pasar desapercibido.*

El titular del Juzgado de instrucción nº 1 de Albacete, que recibió ese oficio dictó un auto de la misma fecha. En él, después de dejar constancia de la presentación de la solicitud, en el primero de los fundamentos de derecho decía que "deduciéndose de lo expuesto que existen fundados indicios de que mediante la intervención y escucha de los teléfonos (...) utilizados por Emilio y Ernesto pueden descubrirse hechos y circunstancias de interés sobre la comisión de un delito de tráfico de drogas en el que [éstos] pudieran estar implicados, es procedente ordenar la intervención solicitada...". El examen de los datos que acaban de reseñarse pone de manifiesto que lo aportado por la policía y que en el auto se califica impropiamente de "fundados indicios" no pasa de ser la mera afirmación de que podría estar cometiéndose un delito, a la que sigue otra, por demás imprecisa, relativa a algún aspecto del supuesto modus operandi.

[381] STEDH de 20 de junio de 2000, Foxley *vs* el Reino Unido.

Debe también tenerse presente que la prórroga ha de adoptarse antes del vencimiento del plazo pues en otro caso, habría vencido la autorización. La decisión de la prórroga de las escuchas unos días después de terminar el plazo de la intervención inicial, únicamente determina la inconstitucionalidad de las escuchas grabadas en los días no cubiertos por la primera autorización[382].

Ha de tenerse en cuenta que la ilegitimidad constitucional de la primera intervención afecta a las prórrogas y a las posteriores intervenciones ordenadas sobre la base de los datos obtenidos en la primera. Ciertamente, el resultado de la intervención telefónica precedente puede proporcionar datos objetivos indiciarios de la existencia de un delito grave, pero la ilegitimidad constitucional de la primera intervención contamina irremediablemente las ulteriores de ella derivadas[383].

En cualquier caso, la prolongación que se convierta en excesiva a través de prórrogas sucesivas llevaría a considerarla desproporcionada e ilegal, ya que no se observaría ni el principio de necesidad ni la mínima lesividad de la medida respecto al derecho fundamental que está siendo limitado.

[382] Sentencia del Tribunal Supremo, Sala Segunda, 1521/1999, de 3 marzo de 2000.

[383] Por todas, sentencias del Tribunal Constitucional 197/2009, de 28 de septiembre; 171/1999, de 27 de septiembre, 299/2000, de 11 de diciembre; 184/2003, de 23 de octubre; 165/2005, de 20 de junio; 253/2006, de 11 de septiembre.

Por el contrario, no transcienden de la condición de meras infracciones procesales, con el alcance y efectos ya señalados, otras irregularidades que no afectan al derecho constitucional al secreto de las comunicaciones y que tan sólo privan de la suficiente fiabilidad probatoria a la información obtenida, por no gozar de la necesaria certeza y de las garantías propias del proceso o por sustraerse a las posibilidades de un pleno ejercicio del derecho de defensa al no ser sometida a la necesaria contradicción. Así, no existe lesión del derecho fundamental, cuando las irregularidades denunciadas, por ausencia o insuficiencia del control judicial, no se realizan en la ejecución del acto limitativo, sino al incorporar a las actuaciones sumariales su resultado (entrega y selección de cintas, custodia de originales o transcripción de su contenido) pues, en tales casos, la restricción del derecho fundamental al secreto de las comunicaciones, llevada a cabo por los funcionarios policiales en los que se delegó su práctica, se ha mantenido dentro de los límites de la autorización.

Esta carencia probatoria, no obstante, podrá ser cubierta por la aportación de otros medios de acreditaciones válidos, incluso por aquellos que tuvieren su origen en las escuchas telefónicas, procesalmente inválidas como medios de prueba pero constitucionalmente útiles como instrumentos de la investigación[384].

[384] "*Mas al ser tales irregularidades procesales posteriores a la adquisición del conocimiento cuya prueba funda la condena, lo conocido gracias a las escuchas puede ser introducido en el juicio oral como elemento de convicción a través de otros medios de prueba que acrediten su contenido , por ejemplo mediante las declaraciones testificales de los funcionarios policiales que escucharon las conversaciones intervenidas"* sentencias del

Asimismo, si por un lado el éxito de la intervención telefónica no subsana la insuficiencia de los indicios previos; a la inversa, que alguno de esos indicios existentes a priori y utilizados para la intervención luego resulten desvirtuados o pierdan potencialidad o se hayan revelado a posteriori como explicables por razones distintas, no es motivo para privar de legitimidad a la injerencia, y no afectará a la validez del Auto, el hecho de que a posteriori se haya podido demostrar que algunos de los datos valorados no eran exactos. La fundabilidad del Auto ha de hacerse mediante un juicio *ex ante*[385].

De igual modo, la no declaración de secreto, pese a poder ser considerada como irregular, no genera defectos insubsanables. En estos supuestos se trataría de una vulneración de la legalidad ordinaria sin ningún alcance constitucional que pueda viciar la validez de este medio de investigación[386].

En este mismo sentido, la sentencia del Tribunal Supremo 402/2008, de 30 de junio, considera que la no declaración de secreto es un vicio de procedimiento sin relevancia constitucional, ya que no existió indefensión material alguna para las personas afectadas (artículo 24.1) que, cuando en calidad de imputados, tomaron contacto con las actuaciones judiciales practicadas, pudieron conocer la medida adoptada

Tribunal Constitucional 228/1997, de 16 de diciembre, FJ 9 y 11 , y 121/1998, de 15 de junio, FJ 5.

[385] Sentencia del Tribunal Supremo, Sala Segunda, 658/2012, de 13 de julio.

[386] Sentencias del Tribunal Supremo, Sala Segunda, 182/2004, de 23 de abril, 9/2004 de 19 de enero y 358/2004 de 16 de marzo; y sentencia del Tribunal Constitucional 100/1995 de 11 de junio.

en secreto contra ellos, su alcance y contenido, y además, tuvieron oportunidad para solicitar al respecto lo que consideraran conveniente para la defensa de sus intereses, no sólo en las calificaciones provisionales, trámite legalmente previsto para pedir la prueba a practicar en el juicio oral, sino incluso durante las diligencias previas antes de su conclusión.

Incluso existe una línea jurisprudencial que defiende que la decisión de proceder a unas intervenciones telefónicas lleva implícita la declaración de secreto de las actuaciones por definición y por elementales exigencias de la lógica (sentencias del Tribunal Supremo, Sala Segunda, 940/2008, de 18 de diciembre, 1090/2005, de 15 de septiembre) pues *"sería absurdo avisar a alguien de que se le va a intervenir su teléfono"* (sentencias del Tribunal Supremo, Sala Segunda, 738/1996, de 11 de octubre). En la misma posición, la sentencia del Tribunal Supremo, Sala Segunda, de 4 de febrero de 2008 recuerda la constante doctrina jurisprudencial que tiene declarado que *"la declaración de secreto de las actuaciones es consecuencia de este medio excepcional de investigación, y que su ausencia solo tiene el alcance de una mera irregularidad procesal que no afecta a la validez de las intervenciones, se suerte que no puede proclamarse ni nulidad de la medida ni indefensión para el sujeto concernido".*

En esta misma línea, la sentencia del Tribunal Supremo, Sala Segunda, 704/2009, de 29 de junio declara que como elemento esencial

implícito a la misma y presupuesto de su efectividad y utilidad, debe entenderse comprendido el secreto de la diligencia de intervención telefónica, y no sólo por la necesidad inmanente de la propia diligencia, sino porque su notificación le privaría de practicidad a la misma, y uno de los condicionamientos de la medida injerencial es su utilidad, y el Juez no puede contradecirse dictando una medida inútil, que por tal razón sería improcedente e inadecuada hasta el punto de arrastrar la nulidad de la misma, y un instructor no dicta conscientemente una medida nula[387].

Se hace preciso recordar que la nueva redacción de la Ley de Enjuiciamiento Criminal impone la declaración de secreto, en su artículo 588bis d, y dictamina que la solicitud y las actuaciones posteriores se sustancien en pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto en la causa. Así, se ha plasmado legalmente la necesidad lógica de actuaciones secretas en esta materia conforme ya defendía, como hemos visto, el Tribunal Supremo, sin que su reflejo normativo suponga mayor gravedad que lo ya expuesto para el caso de incumplimiento; a saber, una mera infracción procesal.

Asimismo, en relación con el uso de modelos de resoluciones judiciales, la sentencia del Tribunal Supremo, Sala Segunda, de 31 de octubre de 1998, dispuso que "*el uso de impresos – en los supuestos de*

[387] En el mismo sentido se pronuncia la sentencia del Tribunal Supremo, Sala Segunda, 1044/2011, de 11 de octubre.

solicitud policial suficientemente detallada- constituye un importante defecto procesal; sin embargo, no incide en el derecho fundamental, porque no produce indefensión alguna a la parte interesada, por cuanto al tener ésta acceso al procedimiento (inmediatamente o cuando se levante, en su caso, el secreto que pudiera haberse acordado), puede conocer a un tiempo el auto de Juzgado y la solicitud policial que le precede y le sirve de fundamento". Por su parte, la sentencia del Tribunal Supremo, Sala Segunda, de 20 de febrero de 1999, rec. 298/1998, y en relación con la utilización de modelos impresos, defiende la suficiente motivación y recuerda que la línea jurisprudencial se ha decantado por su permisibilidad, si bien no es ocioso recomendar que se añadan razonamientos "ad hoc", con objeto de individualizar cada una de la resoluciones adoptadas. Los antecedentes fácticos son variables, en cuanto a los sujetos y circunstancias en las que se adopta la resolución judicial, por ello es conveniente que se plasmen en el apartado correspondiente del auto habilitador de la intromisión en la intimidad, pero no es menos cierto que la opinión mayoritaria, se inclina por convalidar la fundamentación fáctica realizada por remisión al contenido del oficio de la policía judicial, en el que se contienen los detalles y antecedentes por los que se solicita de la decisión judicial.

En lo relativo al sistema SITEL, aparte de lo ya expuesto anteriormente, se plantea la problemática de las recurrentes peticiones de pruebas periciales informáticas sobre este sistema. Así, a este respecto surgió la sentencia del Tribunal Supremo, Sala Segunda, 722/2012, de 2

de octubre; en ella se clarifica la controversia y se declara su no procedencia en base a que *"cuando el Juez ordena una intervención telefónica no impone la utilización de ningún sistema, sino que autoriza los más avanzados o los que en un momento dado utilice la policía judicial, siempre que ofrezcan plenas garantías, como sucede con el sistema SITEL […] que es el que se ha incorporado con carácter general en nuestro ordenamiento […]. En consecuencia, si la doctrina jurisprudencial ya ha estimado que, con carácter general, el sistema SITEL ofrece suficientes garantías para la validez probatoria de las intervenciones que lo utilicen, y teniendo en cuenta que es el sistema de uso habitual en todos los procedimientos judiciales, resulta innecesaria la práctica de una compleja y dilatoria prueba pericial informática para conocer o acreditar las características básicas del sistema, en todos y cada uno de los juicios que se celebran en los Tribunales españoles en los que se aporten como prueba dichas intervenciones, por lo que la decisión del Tribunal sentenciador denegando la prueba propuesta por considerarla superflua con cita expresa de nuestra doctrina jurisprudencial fue correcta y razonable, y debe de ser confirmada".*

Por su parte, la sentencia del Tribunal Supremo, Sala Segunda, 143/2013, de 28 de febrero, resuelve un reto aún más difícil: La defensa consigue que el órgano sentenciador admita una prueba sobre fiabilidad del sistema, en la que, según criterios estadísticos, se llegaba a la conclusión, por el Servicio de Criminalística de la Guardia Civil, de que el riesgo de manipulación o alteración de los 40 discos grabados en el

procedimiento eran tan solo del 5%[388]. Frente a lo que sería un preocupante margen de error en un proceso penal, considera que los conceptos que se manejan de suceso raro o suceso razonable restan trascendencia a tal margen, acudiendo a su vez a las resultas de las conclusiones del informe de inspección realizado por la AEPD sobre el funcionamiento de SITEL.

Conforme al punto 10 de las conclusiones de la Circular 1/2013 de la Fiscalía General del Estado, es ajustada a Derecho la utilización probatoria de las conversaciones grabadas por el sistema SITEL, y ello en tanto la doctrina jurisprudencial ya ha estimado que, con carácter general, el sistema SITEL ofrece suficientes garantías para la validez probatoria de las intervenciones que lo utilicen y, teniendo en cuenta que es el sistema de uso habitual en todos los procedimientos judiciales, resulta innecesaria la práctica de una compleja y dilatoria prueba pericial

[388] RODRÍGUEZ LAÍNZ al comentar esta sentencia manifiesta lo que sigue: *"El margen de error de que habla el mencionado informe corresponde a la posible intervención de un factor humano, como podría ser un error en la transcripción de los dígitos o de similar naturaleza; más allá de una situación de maledicencia o intencionada manipulación. De ahí que se hable expresamente en la sentencia de que tales hechos deben sorprender; y que el hecho de que se produzcan no es debido al azar sino consecuencia de la influencia de causas ajenas a la aleatoriedad del fenómeno. Si examinamos con atención el referido dictamen, que no hace sino centrar el objeto del análisis a las hipótesis de trabajo que se le plantean como prueba pericial, el mismo parte simplemente de unos presupuestos teóricos para manejar ese porcentaje de manipulación de hasta el 5%; y ello como simple hipótesis de trabajo, de la que se deducía que para llegar a ese nivel de error había que trabajar una muestra de al menos 25.036 archivos de audio. Realmente, el argumento estadístico no convence si no se realiza un análisis real conversación por conversación; lo cual es descartado en el propio informe, que a tal nivel estadístico no se dedica a examinar la fiabilidad de las concretas conversaciones que fueran intervenidas en una determinada causa penal. Si ya de por sí partimos de una verdad apodíctica: que todas las conversaciones grabadas analizadas por el informe procedían de SITEL y no de otra fuente, lo que no podemos aceptar es que de buenas a primeras trabajemos con un porcentaje hipotético del 95% para realizar los cálculos. Ni hubo tal margen de error, ni el informe emitido llegó a concluir que pudiera dudarse lo más mínimo de la autenticidad de ninguno de los archivos de audio grabados en los discos facilitados a la autoridad judicial".*

Vid., RODRÍGUEZ LAÍNZ, J. L., *SITEL: nuevas tendencias…*, *op. cit.*

informática para conocer o acreditar las características básicas del sistema.

En cualquier caso, es clarificadora la argumentación de RODRÍGUEZ LAÍNZ[389] al respecto, la cual compartimos íntegramente. Así sostiene que sin necesidad de acudir a estas auditorías de todo el sistema, las cuales podrían ser salvadas por una auditoría interna a intervalos de tiempo regulares, lo cierto es que la prueba en el campo del contraste y adveración de la autenticidad e inalterabilidad de la información obtenida en el curso de una determinada injerencia, es factible, incluso sin necesidad de grandes y desproporcionados esfuerzos que impidieran el normal funcionamiento del sistema. SITEL está dotado de un sistema de control de accesos que permite hacer un seguimiento de las vicisitudes que haya sufrido una determinada carpeta de interceptación, de la cual sí podrían realizarse periciales en las que se valorará el riesgo real de manipulación. Asimismo de esta misma carpeta se conservan intactos contenidos y datos almacenados, que pueden volver a ser descargados y sometidos a cotejo, bajo la fe pública judicial, sin necesidad de recurrir a un Letrado de la Administración de Justicia en el lugar de los centros de recepción de forma permanente; o que pueden ser extraídos desde la misma sede del centro de recepción. Esta misma disponibilidad permite hacer una comparativa entre ficheros correspondientes a datos o conversaciones, y la información que se facilita a la autoridad judicial, permitiendo comprobar la existencia de

[389] RODRÍGUEZ LAÍNZ, J. L., *SITEL. Ibid.*

posibles omisiones de concretas comunicaciones o datos o descargas correspondientes a días determinados, siendo todo ello posible sin necesidad de comprometer el funcionamiento mismo del sistema ni de forzar una auditoría completa cada vez que se cuestione su fiabilidad.

Para GONZÁLEZ LÓPEZ[390] no es exigible que se proceda a una comprobación exhaustiva de la correspondencia del material incorporado al proceso con los originales, aun cuando el acusado la cuestione genéricamente. Sin embargo, sostiene que la exclusión de comprobaciones adicionales solo ha de admitirse cuando el procedimiento e incorporación al proceso presente suficientes garantías de mantenimiento de integridad, lo que en ningún caso, iría en contra de la presunción de inocencia. Por contra, si no se han reunido las garantías suficientes que eliminen cualquier duda de manipulación, ha de operar el principio in dubio pro reo, y deberán ser los acusadores lo que acrediten que no existe alteración alguna, no compartiendo el autor la presunción de autenticidad recogida en la sentencia del Tribunal Supremo, Sala Segunda, 1215/2009, de 30 de diciembre y en sentencias posteriores.

Entiende el autor que el cuestionamiento de la autenticidad del material aportado, si bien puede realizarse en cualquier momento del procedimiento, lo adecuado es hacerlo en el acto del juicio oral, puesto que, de otro modo, se hace descansar la admisibilidad en la diligencia del

[390] GONZÁLEZ LÓPEZ, J. J., "Intervención de las comunicaciones…", *op. cit.*, p. 112.

acusado, defendiendo además que la carga de impugnar la prueba ha de residir en el juicio oral y no en la fase instructora.

III.2.- Valor probatorio

El termino "prueba" trae su origen del latín *probus*, que significa lo bueno, recto, honrado. De modo que lo que resulta probado, es correcto, es lo bueno[391], es lo que corresponde a la realidad.

En el orden jurídico, el significado de la prueba no difiere mucho del estrictamente idiomático, así la prueba en el procedimiento judicial ha de consistir necesariamente en hacer bueno algo, en afirmar que algo es la realidad.

CARNELUTTI[392] define la prueba como el proceso de fijación de los hechos controvertidos por parte del Juez. BANACLOCHE PALAO[393] entiende que la prueba es la actividad, por la que las partes, intentan convencer al Tribunal, de la certeza positiva o negativa de las afirmaciones contenidas en sus respectivos escritos de alegaciones.

---

391 COPPOLA F., *Prova (materia civile)*, en "Il Digesto Italiano", Volumen XIX, parte seconda, p. 872 y ss.

392 CARNELUTTI, F., "La prueba civile", seconda edizione, 1947, Roma, Edizioni dell' Ateno, Traducción Alcalá-Zamora y Castillo, N., Editorial Depalma, Buenos Aires, 1982, p.25 y p. 57.

393 BANACLOCHE PALAO, J., *La prueba en el proceso penal*, en "Aspectos fundamentales del derecho procesal penal", 1ª Edición, Editorial LA LEY, Madrid, febrero 2010.

En cuanto a la valoración de la prueba, en nuestro proceso penal rige el principio de libre valoración de la prueba dispuesto en el artículo 741 de la Ley de Enjuiciamiento Criminal[394]. Ello no ha de ser confundido con la permisión de la arbitrariedad[395], sino que la valoración de la prueba se ha de efectuar según las reglas del criterio racional, de sana crítica o conforme a la lógica[396].

Algunas consecuencias de este principio de la libre valoración de la prueba son:

a) Que el Tribunal tiene la obligación de razonar o motivar el resultado probatorio en su sentencia, es decir, el juzgador tiene que explicar las razones que justifican su convicción. No existe ninguna prueba con un valor superior a otra. Todas son valoradas de acuerdo con un razonamiento lógico, debiendo ser explicado por el Juez en la Sentencia.

[394] Artículo 741 de la Ley de Enjuiciamiento Criminal: *"El Tribunal, apreciando, según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley.*

Siempre que el Tribunal haga uso del libre arbitrio que para la calificación del delito o para la imposición de la pena le otorga el Código Penal, deberá consignar si ha tomado en consideración los elementos de juicio que el precepto aplicable de aquél obligue a tener en cuenta".

[395] Conforme a la RAE, "arbitrariedad" se identifica con *"acto o proceder contrario a la justicia, la razón o las leyes, dictado solo por la voluntad o el capricho".*

[396] La *sana crítica* como criterio de valoración de la prueba trae su origen de la Ley de Enjuiciamiento Civil de 1855, en concreto de su artículo 317, el cual deja al arbitrio prudencial del magistrado el estimar los medios que han de formar parte de su convicción.

b) Ni el Tribunal Supremo ni el Tribunal Constitucional pueden entrar a decidir si las pruebas fueron adecuadamente valoradas o no por el Tribunal de instancia[397].

Así, los datos de geolocalización, una vez sometidos a la valoración judicial, son susceptibles de contribuir a la convicción judicial acerca de la culpabilidad del acusado, encontrándose su eficacia a veces condicionada a la posibilidad de acreditar mediante medios de prueba auxiliares la exactitud de los datos, lo que plantea una problemática especial, debido al carácter de "prueba científica" que caracteriza a la informatoscópica[398].

Precisamente para dejar a un lado la anterior problemática, surgieron los informes periciales de parametrización[399].

Estos informes periciales tienen por objeto la parametrización, entendida como uno de los métodos más precisos usados para la determinación de la ubicación de un dispositivo conectado con las redes de comunicación. Su utilidad consiste en convertirse en prueba de la presencia física de un determinado dispositivo electrónico en un concreto lugar, si bien nunca podrán asegurar que el usuario de ese dispositivo o el titular de la línea se encontrara allí, lo cual habrá de obtenerse, a

[397] La única excepción es el recurso de casación al amparo del artículo 849.2 de la Ley de Enjuiciamiento Criminal o *"cuando haya existido error en la apreciación de la prueba, basado en documentos que obren en autos, que demuestren la equivocación del juzgador sin resultar contradichos por otros elementos probatorios".*

[398] GONZÁLEZ LÓPEZ, J. J, "Los datos de tráfico de las comunicaciones electrónicas…", *op. cit.*, p. 517.

[399] ANTÓN BARBERA, F. y LUIS TUREGANO, J.V., "Policía científica. Volumen 1", 5ª Edición, Editorial Tirant lo Blanch, Valencia, 2012, pp.734 y ss.

través de deducción indiciaria, por el Juzgador, en relación con otras pruebas que se hayan obtenido que así lo corroboren.

En cualquier caso, este informe deberá cumplir los requisitos generales exigidos para las pericias de conformidad con los artículos 456 a 485 de la Ley de Enjuiciamiento Criminal.

En la actualidad son escasos los informes periciales de parametrización que se han elaborado, si bien por razones lógicas de evolución de las tecnologías, su número e importancia irá incrementándose, y más aún si la INTERPOL[400] culmina su proyecto de creación de un Instituto Internacional de Criminalística y Peritajes, donde sin duda estarían incluidos los informes de que los que estamos hablando.

III.3.- Especial referencia a la prueba ilícita

La prueba penal ilícita se refiere a una evidencia obtenida con vulneración de derechos o libertades fundamentales; se le han venido

[400] El nombre oficial de la Organización es "OIPC-INTERPOL". Las siglas oficiales "OIPC" corresponden a "Organización Internacional de Policía Criminal". La palabra "INTERPOL" es una contracción de la expresión inglesa "international police" (policía internacional). Se trata de la mayor organización policial internacional del mundo, que con 190 países miembros, tiene como misión principal lograr la colaboración entre las distintas policías del planeta.

Vid., INTERPOL. Recuperado de: https://www.interpol.int/es (última consulta: 6 de julio de 2016).

asociando diversos efectos en virtud de las diversas teorías que han surgido a su sombra[401].

III.3.A.- Declaración de la ilicitud de la prueba

Si se defiende la tesis de que la ilicitud probatoria debe denunciarse por las partes de forma inmediata a su conocimiento y ser declarada por el órgano judicial igualmente lo antes posible, evitando la producción de cualesquiera efectos, son varios los momentos procesales según ASENCIO MELLADO[402] en los que la declaración de nulidad de la prueba ilícita puede producirse:

a) En la fase de investigación

En primer lugar, el Juez de la Instrucción debe negarse a autorizar la intromisión en los derechos fundamentales cuando la petición de la Fiscalía o de la Policía no contenga los elementos indispensables para forzar la eficacia de un derecho. De igual manera, deberá el Juez decretar

[401] PLANCHAT TERUAL, J. M., *Prueba ilícita. Fundamento y tratamiento*, en "Estudios sobre la prueba penal. Volumen I. Actos de investigación y medios de prueba en el proceso penal: competencia, objeto y límites", 1ª edición, Editorial LA LEY, Madrid, junio 2010.

[402] ASENCIO MELLADO, J. M., *La exclusión de la prueba ilícita en la fase de instrucción como expresión de garantía de los derechos fundamentales,* Diario La Ley, núm. 8009, Sección Doctrina, Ref. D-30, Editorial LA LEY, 25 enero 2013.

de oficio la nulidad, en los casos en que la ley se lo autorice a hacer, siempre que lo haga con anterioridad a la sentencia[403].

Como sostiene CHOZAS[404], el Juez de Instrucción, sobre la base del artículo 311 de la Ley de Enjuiciamiento Criminal, debe rechazar todas las diligencias de prueba que impliquen vulneración de los derechos fundamentales, siendo esta una vía igualmente preconizada por ARMENTA[405], no obstante lo dicho, esta autora acepta que el Juez Instructor pueda declarar la ilicitud de las pruebas infractoras de derechos, expulsándolas del proceso. En el mismo sentido, se expresa SAN MARTÍN CASTRO[406], para quien la ilicitud se debe declarar en cualquier momento en que sea apreciada.

Por las mismas razones, no se podrá incoar procedimiento si la única base para ello es una prueba obtenida con infracción de derechos fundamentales. Igualmente, tampoco procederá la adopción de medidas cautelares si no hay otros elementos distintos que pudieran justificar el

[403] Artículo 240 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial:

"1. La nulidad de pleno derecho, en todo caso, y los defectos de forma en los actos procesales que impliquen ausencia de los requisitos indispensables para alcanzar su fin o determinen efectiva indefensión, se harán valer por medio de los recursos legalmente establecidos contra la resolución de que se trate, o por los demás medios que establezcan las leyes procesales.

2. Sin perjuicio de ello, el juzgado o tribunal podrá, de oficio o a instancia de parte, antes de que hubiere recaído resolución que ponga fin al proceso, y siempre que no proceda la subsanación, declarar, previa audiencia de las partes, la nulidad de todas las actuaciones o de alguna en particular.

En ningún caso podrá el juzgado o tribunal, con ocasión de un recurso, decretar de oficio una nulidad de las actuaciones que no haya sido solicitada en dicho recurso, salvo que apreciare falta de jurisdicción o de competencia objetiva o funcional o se hubiese producido violencia o intimidación que afectare a ese tribunal".

[404] CHOZAS, J. M., *Breve reflexión sobre la prueba ilícita en el proceso penal español*, en "La prueba ilícita en el procedimiento penal", XX Jornadas Iberoamericanas de Derecho Procesal, Volumen I, Editorial CEDMA, México 2007, p. 84.

[405] ARMENTA DEU, T., "La prueba ilícita (Un estudio comparado)", Editorial MARCIAL PONS, Madrid, 2011, p. 149.

[406] SAN MARTÍN CASTRO, Derecho Procesal Penal. T. II, Editorial Grijley, Lima 2003, p. 868 y ss.

fumus boni iuris y tampoco podrá imputarse formalmente a quien solo tiene en su contra un resultado que debe ser considerado ineficaz.

Las partes deben en esta fase utilizar todos los mecanismos que la ley les confiera para oponerse a la realización de actos de investigación contrarios a los derechos fundamentales o instar la nulidad cuando esta posibilidad esté prevista. De esta manera, deben recurrir las resoluciones judiciales que decreten una intromisión indebida en los derechos e instar los recursos procedentes frente a aquellas que decreten medidas cautelares, apertura del procedimiento o imputación sobre la base de actos que infrinjan derechos fundamentales.

El hecho de que no exista un trámite específico, no es óbice para impedir que se utilicen aquellos a través de los cuales pudiera manifestarse una petición, tendente a valorar y producir los mismos efectos y consagrada en otros textos legales. Que la Ley de Enjuiciamiento Criminal no contenga una norma al respecto, no se opone, tampoco, al uso en el proceso penal del cauce del artículo 240 LOPJ, para denunciar nulidades procesales.

De igual modo, deben las partes recurrir las resoluciones de conclusión de la investigación y de apertura de la siguiente fase, y así los diferentes autos que transforman las diligencias previas en los distintos procedimientos que la ley establece (artículo 779 LECrim).

La Fiscalía General del Estado, en su Circular 1/1999, de 19 de diciembre, defiende una posición claramente favorable a la nulidad de la prueba ilícita, tan pronto como se conozca, disponiendo que *"el Fiscal hará todo lo posible para que por el órgano judicial se declare la nulidad de esa actuación y para que tal declaración de nulidad tenga lugar lo antes posible, recobrando así su plena vigencia el derecho fundamental injustamente conculcado"*; sigue con esta misma línea en su Circular 1/2013, de 11 de enero.

b) En la fase intermedia

Las partes deben solicitar el sobreseimiento, y muy especialmente la Fiscalía, cuando la única prueba existente sea ilícita o las que aparezcan sean derivadas de ésta. Del mismo modo, deben abstenerse de proponer pruebas de estas características y han de solicitar que no se reenvíen al juicio oral, diligencias que sean el resultado de pruebas ilícitas.

El órgano judicial debe acordar el sobreseimiento si no existen elementos de juicio bastantes para fundamentar la acusación, lo que equivale a inexistencia de otras pruebas más que las ilícitas. Deberá inadmitir los medios de prueba que sean cauce de actos violatorios de derechos fundamentales.

c) En la fase de juicio oral

En el acto del juicio, al inicio de las sesiones, se deberá alegar por las partes la ilicitud probatoria, a los efectos de obtener la declaración previa de nulidad y evitar que el medio sea practicado.

Si la prueba es practicada, podrá el órgano de enjuiciamiento no valorarla si estima su ilicitud y, si en fin, es tomada en consideración, podrán las partes recurrir la sentencia por medio de los mecanismos que el ordenamiento prevea para lograr su plena ineficacia.

En contraposición a esta tesis de ASENCIO MELLADO, tenemos a GIMENO SENDRA[407], quien defiende, a colación de la doctrina sustentada por el Auto del TSJ Madrid 28/2010, de 25 de marzo, de declaración (caso Gürtel), en la instrucción, de la nulidad de las escuchas telefónicas, que *"... debiera corregirse, si se repara en que la misión de la instrucción no consiste en la declaración de la ilegalidad de los medios de prueba, sino la determinación del hecho punible y la responsabilidad de su autor. El Juez de Instrucción podrá dictar un auto de sobreseimiento en los supuestos en los que la Ley de Enjuiciamiento Criminal le autoriza, pero lo que no se le debiera autorizar es efectuar declaraciones sobre la ilicitud de*

[407] GIMENO SENDRA, V., *Corrupción y propuestas de reforma,* Diario La Ley, núm. 7990, Sección Doctrina, Editorial LA LEY, 26 diciembre 2012.
Posteriormente también en GIMENO SENDRA, V., *La improcedencia de la exclusión de la prueba ilícita en la instrucción (contestación al artículo del Prof. ASENCIO),* Diario La Ley, núm. 8021, Sección Tribuna, Año XXXIV, Ref. D-55, Editorial LA LEY, 12 febrero 2013.

las pruebas. Es ésta una competencia del órgano jurisdiccional decisor, quien, bien en la comparecencia previa, bien en la Sentencia podrá declarar la inconstitucionalidad de tales pruebas, así como la extensión de sus efectos".

Claramente, expone el autor su oposición a que el Juez instructor efectúe declaraciones sobre la ilicitud de las pruebas, por ser ésta una competencia del órgano jurisdiccional decisor quien, bien en la comparecencia previa, bien en la sentencia podrá declarar la ilegalidad de tales pruebas, así como la extensión de sus efectos, entendiendo que la función del Juez de Instrucción no consiste en valorar pruebas, ni en expulsar de su investigación las "ilícitas" y todas las que se deriven de ellas, sino en investigar y recabar la prueba del hecho punible y la responsabilidad de su autor (artículo 299 LECrim.) y, si no existieran indicios racionales de criminalidad, habrá de dictar un Auto de sobreseimiento.

III.3.B.- Determinación de los efectos de la prueba ilícita

Ante la ausencia de legislación, jurisprudencia y doctrina específica en esta materia en relación a los datos de geolocalización, nos basamos en premisas generales, muchas de ellas fijadas a la luz de la intervención de las comunicaciones.

Hay que partir de la idea de que las sentencias condenatorias sustentadas en escuchas telefónicas inconstitucionales, no sólo infringen el artículo 18.3 de la Constitución Española, sino también la presunción de inocencia o el derecho a un proceso con todas las garantías del artículo 24.2, ya que una de las garantías de este derecho fundamental consiste en no ser condenado mediante una prueba obtenida con violación de las normas tuteladoras de los derechos fundamentales.

La interdicción procesal de las pruebas ilícitamente adquiridas se integra en el contenido esencial del derecho a un proceso con todas las garantías (artículo 24.2 de la Constitución Española), en la medida en que la recepción procesal de dichas pruebas implica "una ignorancia de las garantías propias del proceso", comportando también "una inaceptable confirmación institucional de la desigualdad entre las partes en el juicio, desigualdad que se ha procurado antijurídicamente en su provecho quien ha recabado instrumentos probatorios en desprecio de los derechos fundamentales de otro" (STC 261/05)[408].

Hasta el año 1999, la jurisprudencia del Tribunal Constitucional venía subsumiendo el restablecimiento de este derecho a través de la presunción de inocencia. A partir de la Sentencia del Tribunal Constitucional 49/1999 se suele efectuar dicha subsunción dentro del

[408] Sentencias del Tribunal Constitucional 261/2005, de 24 de octubre, FJ 5, que rememora las sentencias del Tribunal Constitucional 49/1999, de 5 de abril FJ 12; 28/2002, de 11 de febrero, FJ 4; 205/2002, de 11 de noviembre, FJ 6, 81/1998, de 2 de abril FJ 3.

derecho a un proceso con todas las garantías[409], si bien existen algunos fallos que todavía lo incluyen en la presunción de inocencia[410].

La disyuntiva anterior no carecía de importancia. Así, si se opta por entenderlo como una infracción de la presunción de inocencia (*vicio in iudicando*), el restablecimiento de este derecho fundamental lo efectúa el propio Tribunal Constitucional mediante la anulación de la sentencia de instancia, lo que equivaldrá a una sentencia absolutoria; mientras que si por el contrario, estimamos que es una infracción del derecho a un proceso con todas las garantías (*vicio in procedendo*), el restablecimiento del derecho no ocasiona la absolución del condenado, sino la nulidad del juicio oral y la retroacción de las actuaciones, a fin de que al inicio de las sesiones, en la comparecencia previa del proceso penal abreviado, el tribunal decida admitir otra prueba válida de cargo propuesta por la acusación, de cuya práctica y valoración dependerá la absolución o condena del acusado.

---

[409] Sentencias del Tribunal Constitucional 171/1999, de 27 de septiembre, 236/1999, de 20 de diciembre, 202/2001, de 15 de octubre, 167/2002, de 18 de septiembre, y 184/2003, de 23 de octubre.

Sentencia del Tribunal Constitucional 236/1999, de 20 de diciembre, FJ 4: *"la práctica totalidad de las irregularidades denunciadas, como antes se dijo, se refieren a la forma en que el resultado de las intervenciones telefónicas ordenadas por el Juez Instructor se incorporaron, primero al sumario y después al juicio oral, y son ajenas al contenido esencial del derecho al secreto de las comunicaciones. Como tiene declarado este Tribunal, no pueden confundirse, en este sentido, los defectos producidos en la ejecución de una medida limitativa de derechos y aquellos otros que acaezcan al documentar o incorporar a las actuaciones el resultado de dicha medida limitativa, ni cabe pretender que uno y otros produzcan las mismas consecuencias. En concreto, no puede existir lesión del art. 18.3 CE, cuando, como ocurre en el presente caso, las irregularidades denunciadas, por ausencia o insuficiencia del control judicial, no se refieren a la ejecución del acto limitativo sino a la forma de incorporar su resultado al proceso (por todas, SSTC 121/1998 y 151/1998)".*

[410] Sentencias del Tribunal Constitucional 50/2000, de 28 de febrero, 299/2000, de 11 de diciembre, 17/2001, de 29 de enero, 138/2001, de 18 de junio y 141/2001, de 18 de junio, y 167/2002, de 18 de septiembre.

En la actualidad, la doctrina mayoritaria es la que individualiza las infracciones del artículo 18.3 CE en el derecho a un proceso con todas las garantías y, si ello es así, ya no cabe, tal y como acontecía con la subsunción en la presunción de inocencia, que el Tribunal Constitucional, a la hora de restablecer el derecho fundamental vulnerado, se limite a anular la sentencia del Tribunal de instancia y se produzca la libre absolución del condenado, sino que, tratándose de un vicio *in procedendo,* lo correcto ha de ser la anulación de la sentencia condenatoria y la retroacción de las actuaciones al inicio del juicio oral para que, previa acusación del Ministerio Fiscal y articulación de nuevos medios de prueba, el Tribunal de instancia pueda, bien apreciar una desconexión de antijuridicidad de otras pruebas distintas a la de los soportes electrónicos y pueda, sobre ellas, fundar válidamente una sentencia de condena, bien, en cualquier otro caso, dictar una sentencia absolutoria.

Para determinar si la infracción del derecho al secreto de las comunicaciones conlleva también la del derecho fundamental a un proceso con todas las garantías, se hace preciso indagar la extensión de los efectos de aquella primera infracción, pues en puridad, cabe la posibilidad de que una sentencia penal no se sustente, por ejemplo ni en la cinta magnetofónica inconstitucionalmente obtenida, ni en pruebas que se deriven de ella (STC 49/96), en cuyo caso la única pretensión de amparo que le puede quedar al particular es meramente declarativa, sin perjuicio de la deducción de la correspondiente denuncia penal y de la

oportuna pretensión resarcitoria que pudiera plantear el destinatario de la escucha ilegal para exigir la reparación de los daños ocasionados por la autoridad pública al haberse entrometido ilegítimamente en su privacidad. Conviene precisar, por tanto, como hace la Sentencia del Tribunal Constitucional 81/1998, del Pleno de este Tribunal, FJ3, que *"la presunción de inocencia, como derecho a no ser condenado sin pruebas de cargo válidas, no puede erigirse, a la vez, en canon de validez de las pruebas: ese canon ha de venir dado por el contenido del derecho a un proceso con todas las garantías ». Y si es cierto que al valorar pruebas obtenidas con vulneración de derechos fundamentales u otras que sean consecuencia de dicha vulneración, puede resultar lesionado, no sólo el derecho a un proceso con todas las garantías, sino también la presunción de inocencia, pero «ello sucederá si la condena se ha fundado exclusivamente en tales pruebas; pero si existen otras pruebas de cargo válidas e independientes, podrá suceder que, habiéndose vulnerado el derecho a un proceso con todas las garantías, la presunción de inocencia no resulte, finalmente, infringida".*

Por tanto, para el caso más frecuente de que dicha ilegítima intromisión, no solo ocasione la vulneración del artículo 18.3 de la Constitución Española, sino también la del artículo 24.2, ya que bien los propios soportes electrónicos, bien las pruebas que se deriven de ellos habrán servido al Tribunal sentenciador para fundamentar una sentencia de condena, se le impone al Tribunal de instancia una delicada misión a

la hora de valorar este resultado probatorio consistente en dilucidar los límites de la valoración prohibida[411].

En este sentido, a fin de determinar la extensión de los efectos de la prueba prohibida en la presunción de inocencia, como es sabido, surgieron y coexisten en el derecho comparado dos grandes tesis, la directa y la refleja o doctrina norteamericana del "fruto del árbol envenenado"[412]. El artículo 11.1º LOPJ se ha inclinado por esta última teoría, según LÓPEZ BARJA, al disponer que *"no surtirán efecto las pruebas obtenidas directa o indirectamente, violentando los derechos o libertades fundamentales"* [413].

Fue a partir de la sentencia 85/1994, de 14 de marzo, cuando el Tribunal Constitucional consagró la doctrina del "fruto del árbol empozoñado", reiterada en múltiples resoluciones posteriores[414], instaurando, por primera vez en nuestro país, la eficacia refleja de la prueba prohibida en lo referente exclusivamente a la valoración de la prueba derivada de las escuchas telefónicas.

---

411 Imaginemos la obtención de datos de geolocalización insertos en una comunicación intervenida, y que los mismos, en el marco de una hipotética investigación de un delito de homicidio, sitúen al acusado en el lugar de comisión de los hechos.

412 Utilizada por vez primera en la Sentencia de la Corte Suprema de los USA Nardone *vs.* United States, 60 S. Ct. 266 y secundada por otras resoluciones, como GOLDSTEIN, 62 S. Ct. 1000, GIORDANO, 94 S. Ct. 1820 o ALDERMANN, 89 S. Ct. 961.

413 GIMENO SENDRA, V., *La intervención de…*, *op. cit.*, p. 15.

414 Sentencias del Tribunal Constitucional 114/1984, de 29 de septiembre, 107/1985, de 7 de octubre, 64/1986, de 21 de mayo, 80/1991, de 15 de abril, 86/1995, de 6 de junio, 181/1995, de 11 de diciembre, 49/1996, de 26 de marzo; Autos del Tribunal Constitucional 248/1996, de 16 septiembre y las sentencias del Tribunal Supremo, Sala Segunda, 6133/1999, de 6 de octubre, 1349/1999, 27 de febrero, 5113/1997,17 de julio, 6258/1998, 27 de octubre y 5496/1996, 14 de octubre.

Sin perjuicio de la existencia en aquél entonces de una doctrina dubitativa al respecto por parte del Tribunal Supremo[415] y del Tribunal Constitucional[416], lo cierto es que el Tribunal Constitucional en dos decisiones, las sentencias 59 y 49/1996 dictadas en los casos De La Hoz Uganda y Bravo Morcillo, volvió a reclamar la vigencia de la teoría de los efectos indirectos o reflejos de la prueba prohibida en las escuchas telefónicas[417].

Autores como GIMENO SENDRA[418] se mostraron conformes con dicha postura defendiendo que si el Tribunal no extendiera los efectos de la prueba prohibida también a los actos de prueba que se deriven de ella, el Ministerio Fiscal y la policía encontrarían siempre un medio de prueba indirecto (así, por ejemplo, a través de la prueba indiciaria surgida con ocasión de la ocupación del cuerpo del delito cuya existencia es conocida a través de la escucha o mediante la declaración testifical del funcionario de policía que efectuó la intervención telefónica, etc.) para introducir en el

[415] Como lo demuestra, por ejemplo, el hecho de que en el año 1995, en tanto que la sentencia del Tribunal Supremo, Sala Segunda, de 23 de enero de 1995 —Ponente: Sr. Martín Pallín— mantuvo la teoría refleja, la de 7 de julio de 1995 —Ponente: Sr. Carrero Ramos— la revisó y se inclinó por la directa.

[416] Sentencia del Tribunal Constitucional 86/1995, de 6 de junio, que declaró la inexistencia de violación del artículo 24, no obstante la ilicitud de las escuchas telefónicas, porque el imputado confesó, en presencia de su Abogado, su participación en el hecho punible, siendo por tanto lícita la valoración de pruebas que, aunque se encuentren conectadas desde una perspectiva natural con "el hecho constitutivo de la vulneración del derecho fundamental por derivar del conocimiento adquirido a partir del mismo", puedan considerarse jurídicamente independientes.

[417] GIMENO SENDRA, V., "La intervención de…", *op. cit.*, p.16.

[418] GIMENO SENDRA, V., "Las intervenciones telefónicas en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo", en Diario La Ley, Sección Doctrina, Ref. D-146, tomo 2, Editorial LA LEY, Madrid 1996, p. 5.

proceso el material de hecho que nunca hubiera podido ser conocido de no haberse vulnerado previamente dicho derecho fundamental.

Entiende el autor que la teoría directa no sólo no evita, sino que puede estimular en la práctica la violación del artículo 18.3 de la Constitución, sin que la mera existencia del delito de escuchas ilegales del entonces artículo 192 bis del Código Penal de 1973 (o los actuales delitos de descubrimiento y revelación de secretos del artículo 197 y siguientes, y delito de interceptación de las comunicaciones o utilización de artificios técnicos de escuchas, con violación de las garantías constitucionales o legales del artículo 536 del Código Penal de 1995) sea suficiente para prevenir o erradicar esta práctica ante las dificultades que se plantean en la prueba de tales hechos punibles como consecuencia de la sofisticación de los medios de interceptación de las comunicaciones.

Defiende ASENCIO MELLADO[419] de manera tajante que la prueba ilícitamente obtenida, con vulneración de derechos fundamentales materiales es plenamente ineficaz conforme a lo establecido en el artículo 11.1 LOPJ, y por tanto que la prueba ilícita no puede producir ningún efecto en el proceso, directo o indirecto, y, al no poder ser degradada a una mera prohibición de valoración, se debe declarar, de inmediato, en cuanto sea conocida, la nulidad de esos medios probatorios. Entiende

[419] *"Sostener vivo un proceso sobre una prueba ilícita y nula atenta a la igualdad de las partes, a la buena fe y al derecho de defensa, toda vez que se obliga al imputado a producir una actividad desproporcionada e innecesaria y se le somete al riesgo de verse expuesto a consecuencias innecesarias y derivadas de su propia actividad defensiva. Mala fe y prepotencia del Estado que se torna en represor y obliga a probar inocencias imponiendo inversiones de la carga de la prueba".*
Vid., ASENCIO MELLADO, J. M., *La exclusión de la prueba ilícita…, op. cit.*

que la prueba ilícita, a diferencia de otros conceptos opera en el momento de la obtención de sus fuentes de prueba, no en el de la práctica del medio, recae sobre derechos materiales, no procesales, es insubsanable, no exige indefensión para ser declarada y produce efectos indirectos no funcionales como la nulidad, sino propios de una derivación material o jurídica tendentes a garantizar la preservación del derecho. Estas notas sirven para destacar su autonomía y muchas veces se confunden en la jurisprudencia generando efectos perversos que, siempre, atentan contra la eficacia de los derechos fundamentales.

ASENCIO MELLADO también critica las corrientes que califica de *"poco respetuosas con los derechos fundamentales",* encarnadas por una línea defendida tanto por doctrina como por jurisprudencia que, según él, implican el riesgo evidente de particularización, de discrecionalidad rayando en la arbitrariedad y que generan inseguridad jurídica, a más de estar en la base de esa voluntad política de controlar el Poder Judicial[420]. Así, pone en el punto de mira la teoría de la conexión de antijuridicidad.

Teoría de la conexión de antijuridicidad

[420] Se une al autor, ECHARRI CASI quien defiende que "*El uso expansivo de estas tesis de aprovechamiento reflejo de la prueba ilícita, que neutralizan el efecto expansivo de la prohibición de valoración de las pruebas inconstitucionalmente obtenidas, podría alentar a una utilización de los procedimientos inconstitucionales puesto que indirectamente producirían efecto.".*

ECHARRI CASI, F. J., *Prueba ilícita: conexión de antijuricidad y hallazgos casuales*, Revista Poder Judicial, núm. 69, Consejo General del Poder Judicial, Madrid, 2003.

Esta teoría, también denominada "prohibición de valoración", supone el establecimiento o determinación de un enlace *jurídico* entre una prueba y otra, de tal manera que, declarada la nulidad de la primera, se produce en la segunda una conexión que impide que pueda ser tenida en consideración por el Tribunal sentenciador a los efectos de enervar la presunción de inocencia del acusado[421].

La prohibición de la prueba constitucionalmente ilícita y de su efecto reflejo tiene como finalidad otorgar, en el ámbito de los procesos jurisdiccionales, el máximo de protección a los derechos fundamentales constitucionalmente garantizados; y al mismo tiempo, en el ámbito específico del proceso penal, ejercer un efecto disuasorio de actuaciones contrarias a las garantías constitucionales por parte de los agentes encargados de la investigación criminal, lo que se ha denominado en el derecho anglosajón *deterrence effect*. La finalidad de la doctrina es de capital importancia a la hora de analizar en cada supuesto si concurre o no conexión de antijuridicidad[422].

La construcción del Tribunal Constitucional, desde la sentencia 81/1998 hasta esta fecha, descansa sobre la "conexión de antijuricidad"[423], doctrina que la sentencia del Tribunal Constitucional

[421] Sentencia del Tribunal Supremo, Sala Segunda, 258/2012, de 30 de octubre.

[422] Circular 1/2013, de la Fiscalía General del Estado, punto 24.

[423] Con la construcción de la doctrina de la conexión de antijuricidad, se fija la competencia para su examen en los Jueces o Tribunales ordinarios, señalando que *"la valoración acerca de si se ha roto o no el nexo entre una prueba y otra no es, en sí misma, un hecho, sino un juicio de experiencia acerca del grado de conexión que determina la pertinencia o impertinencia de la prueba cuestionada que corresponde, en principio, a los*

167/2002 resume así: *"… en aquella sentencia (la STC 81/1998) el Tribunal Constitucional estableció un criterio básico para determinar cuándo las pruebas derivadas de otras constitucionalmente ilegítimas podían ser valoradas o no, que cifró en determinar si, además de estar conectadas desde una perspectiva natural, entre unas y otras existía lo que denominó conexión de antijuridicidad. Para tratar de determinar si esa conexión de antijuridicidad existe o no, se ha de analizar, en primer término, "la índole y características de la vulneración del derecho al secreto de las comunicaciones, materializadas en la prueba originaria, así como su resultado, con el fin de determinar si, desde un punto de vista interno, su inconstitucionalidad se trasmite o no a la prueba obtenida por derivación de aquélla; pero, también, hemos de considerar, desde una perspectiva que pudiéramos denominar externa, las necesidades esenciales de tutela que la realidad y efectividad del derecho al secreto de las comunicaciones exige. Estas dos perspectivas son complementarias, pues sólo si la prueba refleja resulta jurídicamente ajena a la vulneración del derecho y la prohibición de valorarla no viene exigida por las necesidades esenciales de tutela del mismo, cabrá entender que su efectiva apreciación es constitucionalmente legítima, al no incidir negativamente sobre ninguno de los aspectos que configuran el contenido del derecho fundamental*

Jueces y Tribunales ordinarios, limitándose nuestro control a la comprobación de la razonabilidad del mismo".

La tesis anterior ha sido también avalada por autores como JIMÉNEZ SEGADO.

JIMÉNEZ SEGADO, C., *La prueba ilícita y las reglas de "desconexión" de sus efectos*, La Ley Penal, núm. 58, Sección Estudios, Editorial LA LEY, marzo 2009.

sustantivo"[424]. De manera que es posible que la prohibición de valoración de pruebas originales no afecte a las derivadas, si entre ambas, en primer lugar, no existe relación natural o si, en segundo lugar, no se da la conexión de antijuridicidad[425].

El mismo Tribunal Constitucional (STC 166/1999, de 27 de septiembre) ya precisó las razones que avalan la independencia jurídica de unas pruebas respecto de otras, así entendió que la razón fundamental reside en que las pruebas derivadas son, desde su consideración intrínseca, constitucionalmente legítimas, pues ellas no se han obtenido mediante la vulneración de ningún derecho fundamental; por lo tanto, no puede entenderse que su incorporación al proceso implique lesión del derecho a un proceso con todas las garantías. En el caso concreto de la intervención de las comunicaciones, en la medida en que la información obtenida a través de las mismas, incluidos los datos de geolocalización, puede ser incorporada al proceso como medio autónomo de prueba, bien por sí mismo -audición de las cintas o soporte informático-, bien a través de su transcripción mecanográfica -como documentación de un acto sumarial previo-, bien a través de las declaraciones testificales de los funcionarios policiales que escucharon y/o recogieron las conversaciones intervenidas (SSTC 121/1998, de 15 de junio, FJ5 y 151/1998, de 13 de julio FJ4), para que las pruebas

[424] Sentencias del Tribunal Constitucional 11/1981, de 8 de abril, FJ 4 y 8; también, sentencias del mismo órgano 49/1999, de 5 de abril, FJ 14; 166/1999, de 27 de septiembre, FJ 4; 299/2000, de 11 de diciembre, FJ 9.

[425] Sentencias del Tribunal Constitucional 81/1998, 2 de abril, FJ 4, 166/1999, de 27 de septiembre, FJ 4; 171/1999, de 27 de septiembre, FJ 4; 299/2000, de 11 de diciembre, FJ 4; 167/2002, de 18 de septiembre y 66/2009, de 9 de marzo, 197/2009, de 28 de septiembre, FJ 4, y 184/2003, de 23 de octubre, FJ 2, y entre otras, sentencia del Tribunal Supremo, Sala Segunda, 26/2010, de 27 de abril, FJ 2.

derivadas puedan quedar afectadas por la prohibición constitucional de valoración de pruebas ilícitas es preciso que la ilegitimidad de las pruebas originales se transmita a las derivadas (SSTC 81/1998, de 2 de abril, FJ4 y 121/1998, de 15 de junio, FJ6). Esta transmisión se produce en virtud de la existencia de una conexión de antijuridicidad cuya presencia resulta del examen conjunto del acto lesivo del derecho y su resultado, tanto desde una perspectiva interna, es decir, en atención a la índole y características de la vulneración del derecho al secreto de las comunicaciones, como desde una perspectiva externa, a saber, de las necesidades esenciales de tutela exigidas por la realidad y efectividad de este derecho (SSTC 81/1998, de 2 de abril, FJ 4, 121/1998, de 15 de junio, FJ 5 y 49/1999, de 5 de abril, FJ 14).

Para tratar de determinar si esa conexión de antijuridicidad existe o no, se ha de analizar, en primer término, la índole y características de la vulneración del derecho al secreto de las comunicaciones materializadas en la prueba originaria, así como su resultado, con el fin de determinar si, desde un punto de vista interno, su inconstitucionalidad se transmite o no a la prueba obtenida por derivación de aquélla; pero, también se ha de considerar, desde una perspectiva que pudiéramos denominar externa, las necesidades esenciales de tutela que la realidad y efectividad del derecho al secreto de las comunicaciones exige. Estas dos perspectivas son complementarias, pues sólo si la prueba refleja resulta jurídicamente ajena a la vulneración del derecho y la prohibición de valorarla no viene exigida por las

necesidades esenciales de tutela del mismo, podrá entenderse que su efectiva apreciación es constitucionalmente legítima, al no incidir negativamente sobre ninguno de los aspectos que configuran el contenido del derecho fundamental sustantivo[426].

Para establecer si estamos ante un supuesto en que debe aplicarse la regla general a que nos hemos referido o, por el contrario, nos encontramos ante alguna de las hipótesis que permiten excepcionarla, habrá que delimitar si estas pruebas están vinculadas de modo directo a las que vulneraron el derecho fundamental sustantivo, es decir, habrá que establecer si existe o no una conexión de antijuridicidad entre la prueba originaria y las derivadas. Tal valoración nos permitirá deducir si la ilegitimidad constitucional de la primera se ha transmitido o no inexorablemente a las segundas, habiendo fijado, también, la doctrina de este Tribunal unos criterios para determinar si se ha producido esta conexión de antijuridicidad. De conformidad con esta doctrina, habrá el juzgador de examinar con atención la relación de causalidad existente entre el resultado probatorio de la intervención telefónica inconstitucionalmente obtenida y el de los demás medios de prueba, de tal suerte que, para extender su conocimiento a esos otros medios de prueba, habrá de comprobar la ausencia de dicha relación de causalidad

[426] "*Es necesario analizar cada intervención en concreto y señalar en que conversación aparece información relevante para la solicitud de otras intervenciones telefónicas afectantes a otras personas, dado que las posibles irregularidades en intervenciones de las que no se ha obtenido información alguna para conseguir pruebas contra los acusados, no pueden ser tenidas en cuenta como base a una nulidad de las que son independientes, ni tener ninguna trascendencia a la hora de proyectar una posible nulidad sobre el resto de pruebas que se pretende utilizar por la acusación. Por tanto cuando una irregularidad afecta a una intervención de la cual no se han extraído datos relevantes para la investigación, dicha irregularidad no puede influir en el resto de intervenciones"* (Sentencia del Tribunal Supremo, Sala Segunda, 841/2016, de 8 de noviembre, que recuerda la 763/2003, de 30 de mayo).

o de antijuricidad o, dicho en otras palabras, tendrá que acreditarse que el hecho punible se habría probado, en cualquier caso, con independencia de la prueba ilícita obtenida con infracción de la Constitución. De dicha doctrina se infiere que, si el Tribunal hubiera de fundar su convicción sobre otras pruebas, distintas a la de la intervención telefónica, a causa de su ilicitud, habrá de plasmar en la sentencia el *juicio de desconexión* de dichas pruebas con respecto a la escucha telefónica inconstitucional[427].

Por tanto, en primer lugar ha de operarse con la idea de que no es la mera conexión de causalidad la que permite extender los efectos de la nulidad a otras pruebas, sino que debe de darse también la conexión de antijuricidad (Sentencia del Tribunal Supremo, Sala Segunda, 740/2012, de 10 de octubre), y en segundo lugar que la prohibición de valoración de pruebas originales no afectará a las derivadas, si, entre ambas, no existe relación natural o si, no se da la conexión de antijuridicidad (SSTC 299/2000, de 11 de diciembre[428] y 167/2002, de 18 de septiembre).

[427] Sentencia del Tribunal Supremo, Sala Segunda, 262/2005, de 24 de octubre, FJ 5, y sentencias del Tribunal Constitucional de 49/1999, de 5 de abril, FJ 14; 166/1999. de 27 de septiembre, FJ 4; 299/2000, de 11 de diciembre, FJ 9; 167/2002, de 18 de septiembre, FJ 6.

[428] La sentencia del Tribunal Constitucional 299/2000, de 11 de diciembre, sostiene que *"si la prueba refleja resulta jurídicamente ajena a la vulneración del derecho y la prohibición de valorarla no viene exigida por las necesidades esenciales de tutela del mismo, cabrá entender que su efectiva apreciación es constitucionalmente legítima, al no incidir negativamente sobre ninguno de los aspectos que configuran el contenido del derecho fundamental sustantivo. De manera que es posible que la prohibición de valoración de las pruebas originales no afecte a las derivadas, si entre ambas, en primer lugar, no existe relación natural o si, en segundo lugar, no se da la conexión de antijuricidad".*

La conexión causal entre ambas pruebas constituye el presupuesto para poder hablar de una prueba derivada. Sólo si existiera dicha conexión procedería el análisis de la conexión de antijuricidad (cuya inexistencia legitimaría la posibilidad de valoración de la prueba derivada). De no darse siquiera la conexión causal no seria necesaria ni procedente analizar la conexión de antijuricidad, y ninguna prohibición de valoración de juicio recaería sobre la prueba en cuestión (sentencia del Tribunal Constitucional 66/2009 de 9 de marzo). La existencia de un nexo causal entre ambas constituye un requisito necesario pero no suficiente para afirmar la ilicitud constitucional de las pruebas derivadas.

La doctrina ha aportado parámetros interesantes para ponderar si concurre conexión de antijuridicidad, elaborando diversas teorías accesorias que complementan lo anteriormente expuesto partiendo del esquema del sistema judicial estadounidense de la nulidad de la prueba ilícita y su irradiación a la prueba derivada de ésta[429]:

1) La doctrina de la buena fe (*good-faith exception*)[430] fundamenta la desconexión de antijuricidad entre la prueba ilícitamente obtenida con vulneración de derechos fundamentales y

[429] GARCÍA SAN MARTÍN, J., *Las fuentes y medios de prueba ilícitos en el ámbito de la investigación de los delitos de tráfico ilícito de drogas,* La Ley Penal, núm. 108, Sección Práctica Penal, Editorial LA LEY, mayo-junio de 2014.

MARCOS GONZÁLEZ, M., *Doctrina constitucional sobre la prueba ilícita: discrepancias interpretativas*, La Ley Penal, núm. 88, Sección Estudios, Editorial LA LEY, diciembre 2011.

[430] Ha sido aplicada en el sistema judicial español en escasas resoluciones como la sentencia del Tribunal Constitucional 22/2003, Caso Madagán, 241/2012, de 17 de diciembre o por el Tribunal Supremo, Sala Segunda, en sentencias como 373/1999, de 3 de marzo.

la prueba consistente en la declaración testifical de los agentes de las fuerzas y cuerpos de seguridad intervinientes, cuando los mismos actuaron en la práctica de aquélla con buena fe, con la convicción de la licitud de la diligencia y desconociendo la consiguiente lesión de derecho fundamental alguno. Esta doctrina parte de la constatación de situaciones en las que los agentes actúan en un estado de error de prohibición, próximo a la invencibilidad.

2) La doctrina de la fuente independiente (*independent source doctrine*)[431] supone analizar si la prueba procede de una fuente probatoria distinta de aquella otra que vulnera un derecho fundamental. Por esta doctrina se excluye la aplicación del efecto reflejo cuando no queda constatada la vinculación directa entre la diligencia de prueba ilícita y la diligencia o diligencias posteriores; esta desvinculación es real, y no meramente potencial. La aplicación de esta doctrina por la jurisprudencia ha sido muy aislada y ha sido confundida con facilidad con el criterio del descubrimiento inevitable[432], diferenciándose de este en que la prueba independiente se obtiene de una fuente que no guarda relación con la prueba originaria ilícita. Esta doctrina no

[431] Sentencias del Tribunal Constitucional 123/2006, de 24 de abril, y 128/2011, de 18 de julio; o sentencias del Tribunal Supremo, Sala Segunda, 129/2005, de 7 de febrero; 1222/2005, de 17 de octubre; 324/2006, de 21 de marzo; 662/2007, de 9 de julio, 25/2008, de 29 de enero, y 521/2008, de 24 de julio.

[432] Las sentencias del Tribunal Supremo, Sala Segunda, 468/2012, de 11 de junio, y 35/2013, de 18 de enero, mostraron una clara tendencia hacia la confusión con la tesis del descubrimiento inevitable.

plantea, en ningún caso, la reflexión del qué habría sucedido si se hubiera obrado rectamente.

3) La doctrina de la conexión atenuada (*attenuated connection doctrine* o *balancing test*) implica valorar si, pese a la relación causal entre la prueba originaria y la derivada, se aprecia alguna circunstancia que la atenúe, como el transcurso de un período de tiempo suficiente o la concurrencia de actos libres interpuestos[433]. El Tribunal Constitucional considera que para determinar si las informaciones deducidas de pruebas obtenidas, con vulneración de derechos fundamentales (intimidad personal y domiciliaria y correspondencia), han privado al conjunto del proceso de las necesarias garantías y de un proceso equitativo, se ha de atender (aparte de si la concreta prueba tuvo una influencia decisiva en el resultado de la acción penal) a todas las circunstancias de la causa y, en concreto, hay que ver si se han respetado los derechos de defensa y cuál ha sido la calidad e importancia de los elementos en cuestión[434].

[433] Esta tesis ha sido asumida recientemente como criterio valorativo, con auténtica valía como juicio de relevancia del acervo probatorio de cargo, en la sentencia del Tribunal Constitucional 142/2012, de 2 de julio.

[434] RODRÍGUEZ LAÍNZ, J. L., *Exclusionary rules y garantías procesales en el ordenamiento procesal penal español*, Diario La Ley, núm. 8203, Sección Doctrina, Año XXXIV, Ref. D-412, Editorial LA LEY, 2 de diciembre de 2013.

4) La doctrina del descubrimiento inevitable (*inevitable discovery exception*)[435] que analiza si la prueba obtenida con infracción de algún derecho constitucional, hubiera sido, en todo caso, descubierta, de manera que el resultado de la prueba ilícita fuese irrelevante, exigiendo para su examen, por tanto, un juicio de futuro[436]. Precisamente es esto último, el principal inconveniente de esta tesis, dado que cualquier hipótesis sobre el futuro está revestida de incierta probabilidad de acierto, por eso se ha sometido esta regla a dos razonables cautelas: el principio de la prohibición de actuaciones dolosas que tendieran a anticipar la obtención de la evidencia aprovechando una actuación mas rápida aunque ilícita, y la necesaria existencia de una línea de investigación, previa a esa afectación del derecho que hubiera llevado al mismo resultado.

Pese a ello, esta posición es de aplicación presente por la jurisprudencia[437], legitimándose la ruptura del nexo de antijuricidad entre la evidencia obtenida por la prueba ilícita y por ejemplo, la declaración del detenido, imputado/investigado o acusado, en la instrucción o en el acto del juicio oral, siempre y cuando esta última se

[435] Esta doctrina tuvo como punto de arranque Estados Unidos, en el caso *Nx vs Williams, 467 U.S. 431* (1984).

[436] Esta tesis se encuentra en la actualidad plenamente vigente, y así la encontramos en sentencia recientes del Tribunal Supremo, Sala Segunda, tales como la 602/2007, de 4 de julio, 927/2012, de 27 de noviembre o 912/2013, de 4 de diciembre, que la resume con la siguiente afirmación "todo resultado que se hubiera producido aunque una de sus condiciones no se hubiera producido, no es el resultado de esa condición".

[437] Sentencia del Tribunal Supremo, Sala Segunda, 649/2013, de 11 de junio, con cita de otras muchas, como la sentencias del Tribunal Constitucional 136/2006, de 8 de mayo, y las 184/2003, de 23 de octubre, y 161/1999, de 27 de septiembre.

practique en condiciones defensivas adecuadas y advertido aquel de su derecho a no declarar, permitiendo, en consecuencia y a través de ésta, la recuperación procesal de tales hallazgos o evidencias[438].

La diligencia de investigación consistente en la obtención/intervención de los datos de geolocalización, trasladada al proceso como fuente de prueba, ostenta las características básicas y esenciales de cualquier otra que, tras su acceso al juicio oral, se convierte en medio de prueba.

Como no puede ser de otra manera, los debates suscitados en torno a los soportes informáticos como fuente de prueba son de aplicación a esta diligencia, si bien la misma supera todas las exigencias normativas y jurisprudenciales para convertirse en medio de prueba lícito sobre el que fundamentar una hipotética sentencia condenatoria.

[438] Doctrina que el Tribunal Constitucional considera aplicable no sólo a las declaraciones prestadas en el acto del juicio oral, sino también a las realizadas ante el Juzgado de Instrucción, siempre que, por supuesto, se hayan realizado con respeto de esas garantías que la Constitución y las leyes procesales establecen. Posición doctrinal que es, asimismo, sostenida por el Tribunal Supremo, Sala Segunda, en las sentencias 9/2004, de 19 de enero, 1347/2005, de 16 de noviembre, 208/2009, de 6 de marzo o 27/2010, de 25 de enero.

CONCLUSIONES

I

La nueva tecnología y el avance de las comunicaciones han variado la forma de delinquir, y asociado a ello, de investigar al delincuente. Son múltiples las variantes que la técnica pone a nuestra disposición para averiguar la ubicación de una persona a través de señales facilitadas por los satélites que conforman el GPS, mediante la interactuación con estaciones BTS o incluso usando redes *Wifi*, sin olvidarnos de las inmensas bases de datos con las que cuentan los operadores de servicios de telefonía.

Estos instrumentos, de manera aislada o combinada, son utilizados por los ciudadanos en su vida cotidiana, sin ser en muchos casos conscientes; así, al navegar por internet con el ordenador o el *smartphone*, al enviar su ubicación a través de mensajería instantánea a otro interlocutor, al contratar servicios de telefonía o incluso al realizar una fotografía a través de su teléfono móvil.

II

Los datos de geolocalización han sido tratados por la legislación, tanto nacional como europea, de manera sectorial sin darse cuenta de la pluridimensionalidad de su naturaleza, a veces de forma tangencial aprovechando regulaciones de otras materias, y siempre de manera insuficiente. Ello supone que se ha infravalorado su función como medida de investigación y su naturaleza como fuente de prueba, sin que parezca haberse percatado el legislador de la real trascendencia de estos datos, ya que incluso pueden suponer la afectación de un derecho fundamental, como es el derecho al secreto de las comunicaciones previsto en el artículo 18.3 de la Constitución Española.

La jurisprudencia y la doctrina tampoco han tratado los datos de geolocalización como un todo, sino que a tenor de determinados supuestos concretos, se han visto forzados a crear su posición al respecto, siempre superados por la realidad del avance de las tecnologías.

III

Los datos de geolocalización de estaciones base, tratados por operadores de telecomunicaciones, han de ser considerados, como regla

general, como datos de tráfico, pudiendo ostentar también la consideración de datos de suscripción y de datos de servicios de valor añadido, o incluso de dato inserto en la comunicación. La obtención de estos diversos datos de ubicación de la persona se rige, dependiendo de su naturaleza, bien por las reglas de la protección de datos de carácter personal o bien por las normas reforzadas vinculadas con el derecho fundamental al secreto de las comunicaciones.

También es aplicable la normativa prevista para la protección de datos de carácter personal, a los datos de geolocalización procedentes de estaciones base, *WiFi* y GPS tratados por prestatarios de servicios de la sociedad de la información, así como a los obtenidos a través de direcciones IP.

IV

Partiendo de esta pluridimensionalidad de los datos de geolocalización, y habiendo obtenido una clara visión al respecto de su forma de obtención y/o intervención de manera legal y respetuosa con la intimidad y el derecho al secreto de las comunicaciones, en relación con la naturaleza jurídica de cada uno de ellos, se concluye su utilidad procesal dentro del marco de las medidas de investigación y su valoración como fuente de prueba en el proceso penal.

Cuando la medida practicada para su obtención haya sido la intervención de los datos de geolocalización, fuera del contenido propio de la comunicación y con la consideración de datos de tráfico, se precisa la existencia autorización judicial habilitante, de conformidad con el artículo 588 ter d de la Ley de Enjuiciamiento Criminal, tras su reforma operada en octubre del 2015.

Si dichos datos se encuentran ubicados en archivos automatizados de los prestadores de servicios, sin que exista intervención de las comunicaciones, se hace precisa la cesión de la información, en cumplimiento de deber de colaboración, mediando autorización judicial.

Cuando existe una intervención de las comunicaciones, y el dato de localización forma parte de las mismas, hemos de aplicar la regulación prevista para la diligencia de intervención de las comunicaciones telefónicas y telemáticas de los artículos 588 ter a a m de la Ley de Enjuiciamiento Criminal, que sustituyen al obsoleto y criticado derogado artículo 579[439]. Así se podrán intervenir comunicaciones de toda clase, tales como las que incluyan transmisión de fotografías (donde aparecen los archivos *Exif*, que nos informan de la ubicación en la que se hizo la instantánea) o mensajes insertos en aplicaciones de mensajería

[439] RAMOS MENDEZ opina que *"la regulación es tan parca y escueta que mas de una vez se corre el riesgo de que se produzcan atropellos constitucionales"*, mientras que para ANDRÉS IBÁÑEZ esta norma *"plantea mas problemas de los que resuelve"*.

RAMOS MENDEZ, F., "El proceso penal. Lectura constitucional",3ª edición, Bosch Editor, Barcelona, 1993, p.238.

ANDRÉS IBÁÑEZ, P., *Notas sobre la entrada y registro y la intervención telefónica*, en Planes Provinciales y Territoriales de Formación, vol. II, Consejo General del Poder Judicial, Madrid, 1992, p. 1055.

instantánea donde se transmita al interlocutor la ubicación en el espacio. Esta modalidad de intervención de los datos de geolocalización supone el necesario respeto al derecho fundamental de secreto de las comunicaciones, y de los principios de especialidad, idoneidad, especialidad, necesidad y proporcionalidad de la medida.

Por primera vez aparece regulado en la Ley de Enjuiciamiento Criminal, tras su reforma operada por LO 13/2015, el control de los movimientos, desplazamientos y localización de los ciudadanos a través de los dispositivos técnicos de seguimiento o *balizas*, siempre en el marco de una investigación policial. Anteriormente la jurisprudencia ya admitió su existencia y avaló su legalidad, presentándolo como una medida de baja intensidad en cuanto a afectación de la intimidad de la persona afectada.

V

El tratamiento de estos datos, tras su obtención y/o intervención, dentro de la fase de instrucción, también adolece de falta de previsión por parte del legislador. Tras el análisis de la existente norma, surgen numerosas dudas, por ejemplo, en relación a la selección del material obtenido, o a las concretas condiciones en las que debe ser conservado, no solo por parte de los proveedores, sino por el propio Letrado de la

Administración de Justicia (Secretario Judicial), contando únicamente con una insuficiente remisión genérica a la normativa de protección de datos de carácter personal.

VI

Como medio de prueba, esta diligencia de investigación sufre, debido a su naturaleza, las críticas comunes a todos los soportes informáticos. Los sistemas de interceptación de las comunicaciones, por ejemplo SITEL, cumplen con todas las exigencias, anteriormente jurisprudenciales, y recientemente impuestas por la Ley de Enjuiciamiento Criminal, en relación al sistema de sellado o firma electrónica avanzada o sistema de adveración suficientemente fiable, dejando obsoleto el debate al respecto de su autenticidad.

Lógicamente se encuentra sometido como medio de prueba, como no podía ser de otra forma, al trámite procesal de su posible impugnación y en su caso, declaración como prueba ilícita, siendo aplicable, en este supuesto, las previsiones legislativas y jurisprudenciales genéricas en relación a la teoría de la conexión de la antijuricidad.

VII

Con este estudio se ha obtenido un concepto claro de los datos de geolocalización, un análisis de su plural naturaleza jurídica derivada de los múltiples medios técnicos con los que contamos para su obtención tras el desarrollo de la tecnología, así como la determinación clara de la norma aplicable dependiendo de la tipología del dato.

Tras lo anterior, ha quedado patente su valor como medida de investigación, y su peso como fuente de prueba dentro del proceso penal.

BIBLIOGRAFÍA

AUTORES

ANDRADA MÁRQUEZ, L., *Galileo: El sistema europeo de navegación por* satélite, División de Navegación por Satélite. Aeropuertos Españoles y Navegación Aérea (AENA). Recuperado de: http://www.coit.es/archivo-bit/mayo-junio-2001/telecomunicaciones-y-navegacion-por-satelite-galileo-el-sistema-europeo (última consulta: 3 de marzo de 2015).

AGUSTINA, J.R., *Sobre la utilización oculta de GPS en investigaciones criminales y detección de fraudes laborales. Análisis jurisprudencial comparado en relación con el derecho a la intimidad*, La Ley Penal, núm. 102, Sección Estudios, Editorial LA LEY, mayo-junio 2013.

ALCÁCER GUIRAO, R., *Derecho a la intimidad, investigación policial y acceso a un ordenador personal (Comentario a la STC 173/2011, de 7 de noviembre)*, La Ley Penal, núm. 92, Sección Jurisprudencia del Tribunal Constitucional, Editorial LA LEY, abril 2012.

ALZAGA VILLAAMIL, O., "Derecho Político Español según la Constitución de 1978", Editorial Centro de Estudios Ramón Areces, S.A., Madrid 1998.

ANDRÉS IBÁÑEZ, P., *Notas sobre la entrada y registro y la intervención telefónica*, en Planes Provinciales y Territoriales de Formación, vol. II, Consejo General del Poder Judicial, Madrid, 1992.

ANTÓN BARBERA, F. / LUIS TUREGANO, J.V., "Policía científica. Volumen 1", 5ª Edición, Editorial Tirant lo Blanch, Valencia, 2012.

ARMENTA DEU, T., "La prueba ilícita (Un estudio comparado)", Editorial Marcial Pons, Madrid, 2011.

ASENCIO MELLADO, J.M., "Prueba prohibida y prueba preconstituida", Editorial S.A. Trivium, Madrid, 1989.

_____.*La exclusión de la prueba ilícita en la fase de instrucción como expresión de garantía de los derechos fundamentales,* Diario La Ley, núm. 8009, Sección Doctrina, Ref. D-30, Editorial LA LEY, 25 enero 2013.

_____.*Otra vez sobre la exclusión de las pruebas ilícitas en fase de instrucción penal (Respuesta al Prof. Gimeno Sendra),* Diario La Ley, núm. 8026, Sección Doctrina, Año XXXIV, Ref. D-67, Editorial LA LEY, 19 febrero 2013.

AUGUSTI, G., Apéndice a la obra de Carnelutti, "La prueba civile", Edizioni dell' Ateno, Roma, 1947, traducción Alcalá-Zamoran y Castillo, N., Editorial Arayu, Buenos Aires, 1955.

BANACLOCLE PALAO, J., *La prueba en el proceso penal*, en "Aspectos fundamentales del derecho procesal penal", 1ª Edición, Editorial LA LEY, Madrid, febrero 2010.

BARRADO CASADO, M.A., *La captación de datos e intervención de las comunicaciones. Una visión técnico-policial*, en "Interceptación de las comunicaciones y nuevas tecnologías", Cuadernos Digitales de Formación, núm. 43, Consejo General del Poder Judicial, Madrid, 2010.

BENTHAM, J. "Tratado de las pruebas judiciales", Capítulo VI, Libro I. Traducción por OSORIO FLORIT, Ediciones E.J.E.A., Buenos Aires, 1959.

BERNING PRIETO, A. D., *La intervención de las comunicaciones electrónicas*, Revista Aranzadi Doctrinal núm. 3/2012, parte Estudio, Editorial Aranzadi, Pamplona, 2012.

BUENO DE MATA, F., *Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las*

medidas de investigación tecnológica, Diario La Ley, núm. 8627, Sección Doctrina, Ref. D-382, Editorial LA LEY, 19 octubre 2015.

CABEZUDO RODRÍGUEZ, N., *La Administración de Justicia ante las nuevas tecnologías. Del entusiasmo a la desconfianza, pasando por el olvido,* Revista Jurídica de Castilla y León num.7, Administración Pública de Castilla y León, octubre 2005.

CARNELUTTI, F., "La prueba civile", seconda edizione, 1947, Roma, Edizioni dell' Ateno, Traducción Alcalá-Zamora y Castillo, N., Editorial Depalma, Buenos Aires, 1982.

CHOZAS, J. M., *Breve reflexión sobre la prueba ilícita en el proceso penal español*, en "La prueba ilícita en el procedimiento penal", XX Jornadas Iberoamericanas de Derecho Procesal, Volumen I, Editorial CEDMA, México, 2007.

COPPOLA F., *Prova (materia civile)*, en "Il Digesto Italiano" Volumen XIX, parte seconda.

COZAR BARREIRO, J., *Delincuencia informática: conceptos básicos y posibilidades de investigación*, en "Interceptación de las comunicaciones y nuevas tecnologías", Cuadernos Digitales de Formación, núm. 43, Consejo General del Poder Judicial, 2010.

CUADRADO SALINAS, C., *Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa,* La Ley Penal, núm. 107, Sección Estudios, Editorial LA LEY, 2014.

DAVARA RODRÍGUEZ, M. A., *Instrucción penal y nuevas tecnologías,* en "El Juez de instrucción y Juez de garantías: posibles alternativas", Consejo General del Poder Judicial, Madrid, 2002.

DELGADO MARTÍN, J., *La prueba electrónica en el proceso penal,* Diario La Ley, núm. 8167, Sección Doctrina, Año XXXIV, Ref. D-344, Editorial LA LEY, 10 octubre 2013.

_____.*Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos,* Diario La Ley, núm. 8202, Sección Doctrina, Año XXXIV, Editorial LA LEY, 29 noviembre 2013.

DE URBANO CASTRILLO, E., *El documento electrónico: aspectos procesales,* en VV.AA., "Internet y derecho penal", Consejo General del Poder Judicial, Madrid, 2001.

_____.*La investigación tecnológica del delito*, en VELASCO NUÑEZ, E. (Dtor.), "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia", Consejo General del Poder Judicial, Madrid, 2007.

_____.*La prueba electrónica,* La Ley Penal, núm. 46, Sección Estudios, Editorial LA LEY, febrero 2008.

DÍAZ CAPPA, J., *Confidencialidad, secreto de las comunicaciones e intimidad en el ámbito de los delitos informáticos*, Diario La Ley, núm. 7666, Sección Doctrina, Año XXXII, Ref. D-272, Editorial LA LEY, 5 julio 2011.

DÍEZ-PICAZO, L., "Sistema de derechos fundamentales", 1ª Edición, Editorial Civitas, Madrid, 2003.

DOUGLAS E. COMER, *Redes Globales de Información con Internet y TCP/IP*. Recuperado de: http://www.fiuxy.net/ebooks-gratis/1407648-descargar-redes-globales-de-informacion-con-internet-y-tcp-ip-gratis.html (última consulta: 11 diciembre 2015).

ECHARRI CASI, F. J., *Prueba ilícita: conexión de antijuricidad y hallazgos casuales*, Revista Poder Judicial, núm. 69, Consejo General del Poder Judicial, Madrid, 2003.

FERNÁNDEZ-ESPINAR, G., *El levantamiento del secreto de las comunicaciones telefónicas en el marco de las diligencias de investigación y aseguramiento en el proceso penal,* Poder Judicial, núm. 32, Consejo General del Poder Judicial, Madrid, diciembre de 1993.

FERNÁNDEZ LÁZARO, F., *La Brigada de Investigación Tecnológica: la investigación policial*, en VELASCO NÚÑEZ, E. (Dtor.), "Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?", Cuadernos de Derecho Judicial, núm. 3, Consejo General del Poder Judicial, Madrid, 2006.

_____.*Medios técnicos en la investigación de los delitos informáticos*, en VELASCO NÚÑEZ, E. (Dtor.), "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia", Consejo General del Poder Judicial, Madrid, 2007.

FERNÁNDEZ LÓPEZ, J. M., *La protección de datos personales como derecho fundamental en España y en la Unión Europea: su contenido y los derechos que derivan para los ciudadanos*, en "El derecho al honor, a la intimidad y a la propia imagen. El derecho a la libertad frente al uso legítimo de la informática: planteamiento general y problemas civiles", Cuadernos Digitales de Formación, núm. 16, Consejo General del Poder Judicial, Madrid, 2008.

FERRAJOLI, L., "Derecho y razón. Teoría del garantismo penal", 6ª edición, Editorial Trotta, Madrid, 2004.

GARCÍA-GALÁN SANMIGUEL, M. J., *La interceptación de las comunicaciones y su eficacia en el proceso penal*, en "Interceptación de las comunicaciones y nuevas tecnologías", Cuadernos Digitales de Formación, núm. 43, Consejo General del Poder Judicial, 2010.

GARCÍA SAN MARTÍN, J., *Las fuentes y medios de prueba ilícitos en el ámbito de la investigación de los delitos de tráfico ilícito de drogas,* La Ley Penal, núm. 108, Sección Práctica Penal, Editorial LA LEY, mayo-junio de 2014.

GIMENO SENDRA, V. y otros, "Derecho Procesal: proceso penal", Tirant lo Blanch, Valencia, 1993.

GIMENO SENDRA, V., "Las intervenciones telefónicas en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo", Diario La Ley, Sección Doctrina, Ref. D-146, tomo 2, Editorial LA LEY, Madrid, 1996.

_____."Derecho procesal penal", 1ª edición, Editorial COLEX, Madrid, 2004.

_____.*La intervención de las comunicaciones*, Diario La Ley, núm. 7192, Sección Doctrina, Editorial LA LEY, 9 Junio 2009.

_____.*Las intervenciones electrónicas y la policía judicial*, Diario La Ley, núm. 7298, Sección Tribuna, Año XXX, Ref. D-378, Editorial LA LEY, 4 diciembre 2009.

_____.*Corrupción y propuestas de reforma,* Diario La Ley, núm. 7990, Sección Doctrina, Editorial LA LEY, 26 diciembre 2012.

_____.*La improcedencia de la exclusión de la prueba ilícita en la instrucción (contestación al artículo del Prof. ASENCIO),* Diario La Ley, núm. 8021, Sección Tribuna, Año XXXIV, Ref. D-55, Editorial LA LEY, 12 febrero 2013.

_____.*La improcedencia de la exclusión de la prueba ilícita en la instrucción (contestación a la réplica del Prof. ASENCIO),* Diario La Ley, núm. 8027, Sección Tribuna, Año XXXIV, Ref. D-70, Editorial LA LEY, 20 febrero 2013.

GÓMEZ-ANGULO RODRÍGUEZ, M. J., *Limitaciones de derechos fundamentales en la investigación en el proceso penal y las nuevas tecnologías. Entradas y registros en lugar cerrado, intervenciones de comunicaciones y especial referencia a la toma de muestras de ADN.*, Ponencia impartida en el curso "Actuaciones del Juzgado de Guardia. Supuestos procesales y soluciones", Alicante, 22 de marzo de 2012, Plan Territorial de la Comunidad Valenciana, Consejo General del Poder Judicial, 2012.

GONZÁLEZ LÓPEZ, J. J., *Infiltración policial en Internet: algunas consideraciones*, Revista del Poder Judicial, núm. 85, Consejo General del Poder Judicial, Madrid, 2007.

_____."Los datos de tráfico de las comunicaciones electrónicas en el proceso penal", Editorial LA LEY, Madrid, 2007.

_____.*Consideraciones acerca del control de las comunicaciones electrónicas en el ámbito universitario*, en BELLO PAREDES S. y CARO MUÑOZ, A.I. (Dtores) "La Administración electrónica y la protección de datos: encuentro nacional sobre transparencia en la gestión universitaria", Servicio de Publicaciones de la Universidad de Burgos, Burgos, 2009.

_____.*Cesión de datos personales para la investigación penal*, en PÉREZ GIL, J. (Dir.) "Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal", Diario La Ley, núm. 7401, Sección Doctrina, Año XXXI, Editorial LA LEY, 13 mayo 2010.

_____.*Utilización en el proceso penal de datos vinculados a las comunicaciones electrónicas recopilados sin indicios de comisión delictiva*, en "Protección de datos y proceso penal", Editorial LA LEY, Madrid, junio 2010.

_____.*Obtención de la IMSI con fines de investigación penal: Comentario a la STS 248/2008 (Sala de lo Penal, de 20 de mayo)*, Revista Jurídica de Castilla y León, núm. 23, Junta de Castilla y León, enero 2011.

_____.*Infiltración policial en Internet y derechos fundamentales*, Servicio de Publicaciones de la Universidad de Burgos, Burgos, febrero 2011.

_____.*Intervención de las comunicaciones: Nuevos desafíos, nuevos límites*, en PÉREZ GIL, J. (Dtor.) "El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito", Editorial LA LEY, Madrid, 2012.

HERNÁNDEZ GUERRERO, F. J., "La intervención de las comunicaciones electrónicas", III-2001, Estudios Jurídicos, Ministerio Fiscal, 2001.

HERNANDO RABANOS, J. M., "Comunicaciones móviles", 2ª edición, Editorial Universitaria Ramón Areces, Madrid, 2004.

HURTADO ADRIÁN, A. L., *El teléfono como medio de investigación en el proceso penal,* Actualidad Penal, núm. 1, marginal 168, Editorial LA LEY, Madrid,1994.

JIMÉNEZ SEGADO, C., *La prueba ilícita y las reglas de "desconexión" de sus efectos*, La Ley Penal, núm. 58, Sección Estudios, Editorial LA LEY, marzo 2009.

LEAL MEDINA, J., *Ruptura de la cadena de custodia y desconexión con las fuentes de prueba. Supuestos concretos. Reflexiones que plantea,* Diario La Ley, núm. 8846, Sección Doctrina, Ref. D-367, Editorial Wolters Kluwer, 19 octubre 2016.

LÓPEZ-BARJA DE QUIROGA, J., "Las escuchas telefónicas y la prueba ilegalmente obtenida", Editorial Akal, Madrid, 1989.

LÓPEZ, J. y NÁJERA, P., *Los desafíos de seguridad en la Internet de los Objetos,* Revista SIC, vol.88, NICS Lab. Publications, Universidad de Málaga, 2010.

LÓPEZ ORTEGA, J.J., *Contradicción y defensa. Cinco cuestiones sobre la prueba penal, precedidas de una introducción sobre la eficiencia del proceso penal,* en "La generalización del Derecho Penal de excepción: tendencias legislativas", Estudios de Derecho Judicial 128/2007, Consejo General del Poder Judicial, Madrid, 2007.

LUQUE SOTO, R., "Uso policial y análisis forense de información de aplicaciones móviles para localización de personas de interés", (Dtor.) MONTOYA MARTÍ, A., CUGC, Aranjuez, 24 de mayo de 2016.

LLAMAS FERNÁNDEZ, M. Y GORDILLO LUQUE, J. M.*, Medios técnicos de vigilancia*, en VELASCO NÚÑEZ, E. (Dtor.), "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia", Consejo General del Poder Judicial, Madrid, 2007.

MAEZTU LACALLE, D., *La identificación del titular de una dirección IP. Problemática en aplicación de la Ley 25/2007, de conservación de datos*, en PÉREZ GIL, J. (Dtor.) "El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito", Editorial LA LEY, Madrid, 2012.

MARCOS GONZÁLEZ, M., *Doctrina constitucional sobre la prueba ilícita: discrepancias interpretativas*, La Ley Penal, núm. 88, Sección Estudios, Editorial LA LEY, diciembre 2011.

MARCHENA GÓMEZ, M., *Algunos aspectos procesales de Internet,* Cuadernos de Derecho Judicial, núm. 4, Consejo General de Poder Judicial, Madrid, 2000.

_____.*Dimensión jurídico-penal del correo electrónico,* Diario La Ley, núm. 6475, Sección Doctrina, Ref. D-114, Editorial LA LEY, 4 mayo 2006.

_____.*La incorporación al proceso penal de los datos electrónicos en poder de las operadoras de telefonía*, en "Encuentro de la Sala Segunda del Tribunal Supremo con jueces y magistrados del orden penal:

jurisprudencia penal", Cuadernos Digitales de Formación, núm. 35, Consejo General de Poder Judicial, 2009.

_____.*Proceso penal: nuevos problemas, viejas soluciones,* La Ley Penal, núm. 100, Sección Estudios, Editorial LA LEY, Madrid, 2013.

MARTÍNEZ GINESTA, G., *Límites técnicos de la ayuda prestada por las operadoras en la investigación de los delitos,* en VELASCO NÚÑEZ, E., "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia", Consejo General del Poder Judicial, Madrid, 2007.

MAZA MARTÍN, J.M., *La intervención judicial de las comunicaciones a través de Internet*, en "Internet y Derecho Penal", Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2001.

MESEGUER GONZÁLEZ, J. D., *Derechos fundamentales afectados por la geolocalización,* Tribuna, EL DERECHO, 22 julio 2013.

MOLINS GARCÍA-ATANCE, J., *Impugnación y autenticidad documental,* Diario La Ley, núm. 6143, Editorial LA LEY, diciembre 2004.

MONTERO AROCA, J., "La prueba en el proceso penal", 2ª edición, Editorial Civitas, Madrid, 1998.

_____."La intervención de las comunicaciones telefónicas en el proceso penal: un estudio jurisprudencial", Editorial Tirant lo Blanch, Valencia, 1999.

_____."Derecho jurisdiccional II. Proceso civil", edición 16ª, Editorial Tirant lo Blanch, Valencia, 2008.

NARVAEZ RODRÍGUEZ, A., *Escuchas telefónicas: alcance constitucional y procesal,* núm. 1, Revista del Ministerio Fiscal, Madrid, 1995.

_____.*Intervenciones postales,* Estudios Jurídicos del Ministerio Fiscal, VI, Madrid, 1997.

NIETO MARTÍN. A., *Redes sociales en Internet y "Data Mining" en la prospección e investigación de comportamientos delictivos,* en "Derecho y redes sociales", Editorial Civitas, Madrid, 2010.

ORTIZ LÓPEZ, P., *Redes sociales: funcionamiento y tratamiento de información personal*, en "Derecho y Redes Sociales", Editorial Civitas, Madrid, 2010.

PLANCHAT TERUAL, J. M., *Prueba ilícita. Fundamento y tratamiento*, en "Estudios sobre la prueba penal. Volumen I. Actos de investigación y medios de prueba en el proceso penal: competencia, objeto y límites", 1ª edición, Editorial LA LEY, Madrid, junio 2010.

PÉREZ GIL, J., *Convenio de Asistencia Judicial penal*, en JIMENO BULNES, M. (Dtor.), "La cooperación judicial civil y penal en el ámbito de la Unión europea: instrumentos procesales", Editorial BOSCH, Barcelona, 2008.

_____.*Los datos sobre localización geográfica en la investigación penal*, en "Protección de datos y proceso penal", 1ª edición, Editorial LA LEY, Madrid, junio 2010.

_____.*Usos delictivos no comunicativos de la telefonía móvil*, en PÉREZ GIL, J. (Dtor.) "El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito", Editorial LA LEY, Madrid, 2012.

_____.*El nuevo papel de la telefonía móvil en el proceso penal: ubicación y perfiles de desplazamiento*, en PÉREZ GIL, J. (Dtor.) "El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito", Editorial LA LEY, Madrid, 2012.

RAMOS MENDEZ, F., "El proceso penal. Lectura constitucional",3ª edición, Bosch Editor, Barcelona, 1993.

RICHARD GONZÁLEZ, M., *La competencia del Ministerio Fiscal para la investigación de actos delictivos. Diligencias preliminares y competencias de instrucción en el procedimiento de menores*, en "Estudios sobre la prueba penal. Volumen I. Actos de investigación y medios de prueba en el proceso penal: competencia, objeto y límites", 1ª edición, Editorial LA LEY, Madrid, junio 2010.

_____.*Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización,* Diario

La Ley, núm. 8808, Sección Tribuna, Ref. D-292, Editorial LA LEY, 21 julio 2016.

RIFÁ SOLER, J. M., *Actos de investigación, actos de instrucción y actos de prueba*, en "Estudios sobre la prueba penal. Volumen I. Actos de investigación y medios de prueba en el proceso penal: competencia, objeto y límites", 1ª edición, Editorial LA LEY, Madrid, junio 2010.

RIVES SEVA, A. P., "La intervención de las comunicaciones en la jurisprudencia penal", Aranzadi, Madrid, 2000.

_____."La intervención de las comunicaciones en el proceso penal. Análisis doctrinal, legislación y jurisprudencia", Bosch, Barcelona, 2010.

RODRÍGUEZ FERNÁNDEZ, R., *Prueba preconstituida y prueba anticipada. Análisis jurisprudencial,* Diario La Ley, núm. 8487, Sección Doctrina, Ref. D-68, La Ley Penal, Editorial LA LEY, 24 febrero 2015.

RODRÍGUEZ LAÍNZ, J. L., "La intervención de las comunicaciones telefónicas", Bosch, Barcelona, 2002.

_____."La intervención judicial en los datos de tráfico de las comunicaciones", Editorial BOSCH, Barcelona, 2003.

_____."Juzgado de Violencia sobre la Mujer y Juzgado de Guardia", Bosch, Barcelona, 2006.

_____.*Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas*, Diario LA LEY, núm. 7086, Sección Doctrina, Año XXIX, Editorial LA LEY, 2 enero de 2009.

_____.*Consideraciones jurídicas en torno a la licitud constitucional del SITEL*, en Diario La Ley, núm. 7544, Sección Doctrina, Año XXXI, Editorial LA LEY, 17 febrero 2010.

_____.*La fuente de conocimiento del número de terminal objeto de intervención telefónica*, Diario La Ley, núm. 7371, Sección Doctrina, Ref. D-108, Año XXXI, Editorial LA LEY, 29 marzo 2010.

_____.*Incautación policial de teléfonos móviles y secreto de las comunicaciones*, Diario La Ley, núm. 7536, Sección Doctrina, Ref. D-407, Año XXXI, Editorial LA LEY, 28 diciembre 2010.

_____."Estudios sobre el secreto de las comunicaciones. Perspectiva doctrinal y jurisprudencial", 1ª edición, Editorial LA LEY, Madrid, 2011.

_____.*Sobre la dimensión privada y familiar del derecho al secreto de las comunicaciones*, Diario La Ley, núm. 7598, Sección Doctrina, Año XXXII, Ref. D-134, Editorial LA LEY, 28 marzo 2011.

_____.*Sobre la naturaleza formal del derecho al secreto de las comunicaciones: dimensión constitucional e histórica*, Diario La Ley, núm. 7647, Sección Doctrina, Año XXXII, Ref. D-237, Editorial LA LEY, 8 junio 2011.

_____.*Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas*, en "Estudios sobre el secreto de las comunicaciones. Perspectiva doctrinal y jurisprudencial", 1ª edición, Editorial LA LEY, Madrid, diciembre 2011.

_____.*Hacia un nuevo entendimiento de la protección integral de los dispositivos privados de almacenamiento electrónico de datos relativos a las comunicaciones (Comentario a la STC 173/2011, de 7 de noviembre)*, Revista del Ilustre Colegio de Abogados de Madrid, Otrosí, 5ª Época, núm. 9, ICAM, enero-marzo 2012.

_____.*Hacia un nuevo entendimiento del concepto de gravedad del delito en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas*, Diario La Ley, núm. 7789, Sección Doctrina, Año XXXIII, Ref. D-49, Editorial LA LEY, 2 febrero 2012.

_____.*Las bases de datos comerciales relativas a las comunicaciones electrónicas como fuente probatoria en el proceso penal,* Diario La Ley, núm. 7839, Sección Doctrina, Año XXXIII, Editorial LA LEY, 17 abril 2012.

_____.*Los dispositivos electrónicos de posicionamiento global (GPS) en el Proceso Penal*, Diario La Ley, núm. 7945, Sección Doctrina, Ref. D-358, Editorial LA LEY, 17 octubre 2012.

_____.*Internet de los objetos y secreto de las comunicaciones*, Diario La Ley, núm. 8034, Sección Doctrina, Año XXXIV, Ref. D-85, Editorial LA LEY, 1 marzo 2013.

_____.*La interceptación de las comunicaciones telefónicas y telemáticas en el borrador de Anteproyecto de Código Procesal Penal*, Diario La Ley, núm. 8039, Sección Doctrina, Año XXXIV, Ref. D-94, Editorial LA LEY, 8 marzo 2013.

_____.*SITEL: nuevas tendencias, nuevos retos*, Diario La Ley, núm. 8082, Sección Doctrina, Año XXXIV, Editorial LA LEY, 14 mayo 2013.

_____.*El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre*, Diario La Ley, núm. 8122, Sección Doctrina, Año XXXIV, Editorial LA LEY, 9 julio 2013.

_____.*Exclusionary rules y garantías procesales en el ordenamiento procesal penal español*, Diario La Ley, núm. 8203, Sección Doctrina, Año XXXIV, Ref. D-412, Editorial LA LEY, 2 diciembre 2013.

_____.*Reflexiones sobre los nuevos contornos del secreto de las comunicaciones (Comentario a la STC 170/2013, de 7 de octubre)*, Diario La Ley, núm. 8271, Sección Doctrina, Año XXXV, Ref. D-83, Editorial LA LEY, 14 marzo 2014.

_____.*Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre la conservación de datos relativos a las comunicaciones*, Diario La Ley, núm. 8308, Sección Doctrina, Ref. D-148, La Ley Unión Europea, Editorial LA LEY, 12 mayo 2014.

_____.*GPS y balizas policiales*, Diario La Ley, núm. 8416, Sección Doctrina, Año XXXV, Ref. D-369, Editorial LA LEY, 7 noviembre 2014.

_____.*La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto de reforma de la Ley de Enjuiciamiento Criminal de 5 de diciembre de 2014*, Diario La Ley, núm. 8465, Sección Doctrina, Ref. D-27, La Ley Penal, Editorial LA LEY, 23 enero 2015.

ROMEO CASABONA, C. M., *Los perfiles de ADN en el proceso penal: novedades y carencias del Derecho español,* en "Las reformas procesales", Consejo General del Poder Judicial, Madrid, 2005.

_____.*De los delitos informáticos al Cibercrimen. Una aproximación conceptual y político-criminal*, en "El Cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político criminales", Editorial Comares, Granada, 2006.

RUBIO ALAMILLO, J., *Conservación de la cadena de custodia de una evidencia informática,* Diario La Ley, núm. 8859, Sección Doctrina, Ref. D-389, Editorial Wolters Kluwer, 9 noviembre 2016.

SANCHÍS CRESPO, C., "La prueba por soportes informáticos", Editorial Tirant lo Blanch, Valencia, 1999.

SANCHÍS CRESPO, C. y CHAVELI DONET, E. A., "La prueba por medios audiovisuales e instrumentos de archivo en la LEC 1/2000 (Doctrina, jurisprudencia y formularios)", Editorial Tirant lo Blanch, Valencia, 2002.

SAN MARTÍN CASTRO, Derecho Procesal Penal. T. II, Editorial Grijley, Lima, 2003.

SENTÍS MELENDO, S., *La prueba*, en "Los grandes temas del derecho probatorio", Ediciones Jurídicas Europa-América, Buenos Aires, 1979.

TYSON, J., *How Instant Messaging Works*. Recuperado de: http://computer.howstuffworks.com/e-mail-messaging/instant-messaging.htm (última consulta: 12 febrero 2015).

URBANO CASTRILLO, E., *La prueba ilícita penal y el derecho de defensa,* Diario La Ley, Sección Doctrina, Ref. D-149, tomo 3, Editorial LA LEY, Madrid, 1998.

VALLÉS CAUSADA, L. M., "La policía judicial en la obtención de inteligencia sobre comunicaciones electrónicas para el proceso penal", Tesis Doctoral, (Dtor.) DÍAZ MARTÍNEZ, M., UNED, Madrid, diciembre 2012. Recuperado de: http://e-spacio.uned.es/fez/eserv/tesisuned:Derecho-Lmvalles/Documento.pdf

_____.*Usos delictivos no comunicativos de la telefonía móvil: ¿una excepción a la protección del artículo 18.3 CE?*, en PÉREZ GIL, J. (Dtor.) "El proceso penal en la sociedad de la información. Nuevas

tecnologías para investigar el delito", Editorial LA LEY, Madrid, 2012.

VELASCO NÚÑEZ, E., *Presencias y ausencias (aspectos aclarados y discutidos) en materia de intervenciones telefónicas, en espera de una regulación parlamentaria del tema*, Actualidad Penal, núm. 18/3, Editorial LA LEY, 9 mayo 1993.

_____.*Aspectos procesales de la investigación y de la defensa de los delitos informáticos*, Diario La Ley, núm. 6506, Sección Doctrina, Año XXVII, Ref. D-150, Editorial LA LEY, 16 junio 2006.

_____.*Cuestiones procesales relativas a la investigación de los delitos telemáticos*, en VELASCO NÚÑEZ, E. (Dtor.), "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia", Consejo General del Poder Judicial, Madrid, 2007.

_____.*Eliminación de contenidos ilícitos y clausura de páginas web en Internet (medidas de restricción de servicios informáticos)*, en VELASCO NÚÑEZ, E. (Dtor.), "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia", Consejo General del Poder Judicial, Madrid, 2007.

_____.*Correo electrónico, SMS y «virus troyanos»*, Cuadernos Digitales de Formación, núm. 22, Consejo General del Poder Judicial, Madrid, 2009.

_____.*Crimen organizado, Internet y nuevas tecnologías*, en "Crimen Organizado", Cuadernos Digitales de Formación, núm. 42, Consejo General del Poder Judicial, 2010.

_____."Delitos cometidos a través de Internet. Cuestiones procesales", 1ª edición, Editorial LA LEY, Madrid, junio 2010.

_____.*Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías*, Revista de Jurisprudencia, núm. 4, Editorial EL DERECHO, Madrid, 24 febrero 2011.

_____.*Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica,* Diario La Ley, núm. 8183, Sección Doctrina, Año XXXIV, Editorial LA LEY, 4 noviembre 2013.

_____.*La prueba pericial*, Diario La Ley, núm. 8258, Sección Doctrina, Año XXXV, Editorial LA LEY, 25 febrero 2014.

_____.*Tecnovigilancia, geolocalización y datos: aspectos procesales penales*, Diario La Ley, núm. 8338, Sección Doctrina, Año XXXV, Editorial LA LEY, 23 junio 2014.

INSTITUCIONES/ORGANISMOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Recuperado de: https://www.agpd.es/portalwebAGPD/index-ides-idphp.php (última consulta: 12 de enero 2016).

_____.Informe 0247/2008 de la AEPD, Recuperado de: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2008-0247_Acceso-por-el-empresario-al-correo-electr-oo-nico-de-los-trabajadores.pdf (última consulta: 12 abril 2015).

AGENCIA ESTATAL DE SEGURIDAD AÉREA, *Programas de navegación aérea. Cospas-Sarsat*. Ministerio de Fomento. Gobierno de España. Recuperado de:

http://www.seguridadaerea.gob.es/lang_castellano/navegacion/programas/cospas/descripcion/default.aspx (última consulta: 4 de abril 2016).

COMISIÓN EUROPEA, Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, "Hacia un nuevo marco para la infraestructura de comunicaciones electrónicas y los servicios asociados. Revisión de 1999 del sector de las comunicaciones", de 10 de noviembre de 1999.

_____.Comunicación de la Comisión al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, "Comunicación sobre las redes y la Internet del futuro", (COM/2008/594 final), de 29 de septiembre de 2008. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Asi0003 (última consulta: 17 julio 2015).

_____.Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones "Internet de los objetos – Un plan de acción para Europa", (COM (2009/278) final), de 18 de junio de 2009. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Asi0009 (última consulta: 12 diciembre 2016).

_____.Libro Verde sobre la obtención de pruebas en materia penal en otro Estado miembro y sobre la garantía de su admisibilidad, COM(2009)624 final, de 11 noviembre de 2009.

_____.Informe de evaluación sobre la Directiva de conservación de datos, de la Comisaria de Asuntos de Interior, Dª. Cecilia Malmström, de 18 de abril de 2011.

_____.Recomendación de la Comisión de 9 de marzo de 2012, relativa a los preparativos para el despliegue de los sistemas de contador inteligente.

_____.Comisión Europea. Programa Galileo. Recuperado de: http://cordis.europa.eu/programme/ren/871_es.html (última consulta: 2 noviembre 2016).

CONFERENCIA MINISTERIAL G-8, Principles on Transborder Access to Stores Computer Data, Moscú, 19 y 20 octubre 1999. Recuperado de:http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf (última consulta: 5 diciembre 2016).

CONSEJO EUROPEO, Conclusiones de Tampere de la Presidencia del Consejo Europeo de 15 y 16 de octubre de 1999, apartado VI. Recup. de: http://www.europarl.europa.eu/summits/tam_es.htm (última consulta: 12 noviembre 2016).

CONSEJO DE EUROPA, Decisión Marco de Consejo de Europa 2003/577/JHA de 22 de julio de 2003, relativa a la ejecución de medidas cautelares de embargo o aseguramiento de la prueba, incorporada al Derecho español con la Ley 18/2006, de 5 de junio, para la eficacia en la Unión Europea de las resoluciones de embargo y de aseguramiento de pruebas en procedimientos penales, BOE, núm. 134, 6 de junio de 2006.

_____.Decisión Marco 2008/978/JHA de 18 de diciembre de 2008, relativa a la orden europea para la obtención de objetos, documentos y datos dentro del proceso penal, Orden de Obtención de Pruebas Europea.

_____."Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano", aprobado en Bruselas, 2 de diciembre de 2009.

_____.Convenio sobre la Ciberdelincuencia, hecho en Budapest, 23 de noviembre de 2001, BOE, núm. 226, 17 de septiembre de 2010.

FISCALÍA GENERAL DEL ESTADO, Consulta 1/1999 de la Fiscalía General del Estado, de 22 de enero, sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones.

_____.Circular 1/1999, de la Fiscalía General del Estado, de 29 de diciembre, sobre la intervención de las comunicaciones telefónicas en el seno de los procesos penales.

_____.Circular 1/2013 de la Fiscalía General del Estado, de 11 de enero, sobre pautas en relación con la diligencia de intervención de las comunicaciones electrónicas.

_____.Instrucción 2/2008 de la Fiscalía General del Estado, sobre las funciones del Fiscal en la fase de Instrucción.

_____.Memoria, Ministerio de Justicia, 2014.

GRUPO ASESOR DEL PROGRAMA DE TECNOLOGÍAS DE LA SOCIEDAD DE LA INFORMACIÓN (ISTAG), informe "Una aproximación a algunos elementos de Internet de las cosas", 10 febrero de 2009.

MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL, Informe del Grupo Asesor del programa de Tecnologías de la Sociedad de la Información (ISTAG, febrero de 2009).

INSTITUTO GEOGRÁFICO NACIONAL. Recuperado de: http://www.ign.es/ign/layoutIn/faimgsatsatelite.do (última consulta: 16 marzo 2014).

INTERNATIONAL TELECOMMUNICATION UNION. *The Internet of Thing.* ITU Internet Report, noviembre de 2005. Recuperado de: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf (última consulta: 6 marzo 2015).

INTERPOL. Recuperado de: https://www.interpol.int/es (última consulta: 6 julio 2016).

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO, Orden ITC/110/2009, de 28 de enero, en relación a los requisitos y las especificaciones técnicas que resultan necesarios para el desarrollo del capítulo II del título V del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios aprobado por Real Decreto 424/2005, de 15 de abril. BOE núm. 29, de 3 de febrero de 2009.

_____.Orden ITC/313/2010, de 12 de febrero, por la que se adopta la especificación técnica ETSI TS 101 671 "Interceptación legal (LI), Interfaz de traspaso para la interceptación legal del tráfico de telecomunicaciones". BOE núm. 43, de 18 de febrero de 2010.

_____.Orden ITC/682/2010, de 9 de marzo, por la que se adopta la especificación técnica ETSI TS 133 108 (3GPP TS 33.108) "sistema de telecomunicaciones móviles universales (UMTS); LTE; seguridad 3G; interfaz de traspaso para la interceptación legal (LI)". BOE núm. 68, de 19 de marzo de 2010.

_____.Orden IET/2530/2012, de 19 de noviembre, por la que se adoptan varias de las partes de la especificación técnica ETSI TS 102 232 «Interceptación Legal (IL); Interfaz de traspaso y detalles específicos de servicio (SSD) para la entrega mediante el protocolo IP». BOE núm. 285, de 27 de noviembre de 2012.

PARLAMENTO EUROPEO, Decisión 676/2002/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, sobre un marco regulador de la política del espectro radioeléctrico en la Comunidad Europea.

_____.Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

_____.Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

_____.Directiva 2002/19/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión ("Directiva sobre acceso").

_____.Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas ("Directiva sobre autorización").

_____.Directiva 2002/21/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.

_____.Directiva 2002/22/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas ("Directiva sobre servicio universal").

_____.Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas -*Directiva sobre la privacidad y las comunicaciones electrónicas*-, DOUE, núm. 201, de 31 de julio de 2002.

_____.Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, DOUE, núm. 105, de 13 de abril de 2006.

____.Directiva 2009/114/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, por la que se modifica la Directiva 87/372/CEE, de 25 de junio de 1987, relativa a las bandas de frecuencia a reservar para la introducción coordinada de comunicaciones móviles terrestres digitales, celulares públicas paneuropeas en la Comunidad

____.Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) 2006/2004 sobre la cooperación en materia de protección de los consumidores

_____.Directiva 2009/140/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas

_____.Directiva 2012/27/UE, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, relativa a la eficiencia energética, por la que se modifican las Directivas 2007/127/CE y 2010/30/UE, y por la que se derogan las Directivas 2004/8/CE y 2006/32/CE

_____.Directiva 2014/41/CE del Parlamento Europeo y del Consejo, relativa a la orden europea de investigación en materia penal, DOUE, núm. 130, de 1 de mayo de 2014.

REAL ACADEMIA ESPAÑOLA. Diccionario de la Lengua Española. Recuperado de: http://www.rae.es (última consulta: 14 mayo 2013).

REDACCIÓN EDITORIAL LA LEY, *Los smartphones, nuevo talón de Aquiles de la privacidad*, Diario La Ley, núm. 8010, Sección Tribuna, Ref. D-31, Editorial LA LEY, 28 enero 2013.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, Recuperado de: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS?lang=es (última consulta: 9 de diciembre de 2015).

_____.Dictamen del Supervisor Europeo de Protección de Datos sobre la neutralidad de la red, la gestión del tráfico y la protección de la intimidad y los datos personales, DOUE 2012/C 34/01.

SUPREME COURT OF THE UNITED STATES. Recuperado de: https://www.supremecourt.gov (última consulta: 17 de febrero de 2014).

TRIBUNAL SUPREMO, Acuerdo del Pleno, de la Sala Segunda, del Tribunal Supremo, de 23 de febrero de 2010, en relación a la

necesidad de autorización judicial para la obtención de datos conservados por los operadores de telecomunicaciones.

UNIÓN EUROPEA, Convenio de asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, hecho en Bruselas el 29 de mayo de 2000, BOE núm.247, 15 octubre 2003.

_____. Informe de evaluación sobre la Directiva de Conservación de Datos, elaborado el 18 de abril de 2011 por la Comisaria de Asuntos de Interior de la Unión Europea, D.ª Cecilia Malmström. Recuperado de: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2011)0225_/com_com(2011)0225_es.pdf (última consulta: 6 abril 2015).

UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 de la Directiva 95/46/CE, Dictamen 4/2007, del 20 de junio, sobre el concepto de datos personales.

_____.Dictamen 13/2011, de 16 de mayo de 2011, sobre los servicios de geolocalización en dispositivos móviles inteligentes.

_____.Documento de trabajo *Privacidad en Internet: Enfoque comunitario de la protección de datos en línea*, de 21 de noviembre de 2000. Recuperado de: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37es.pdf (última consulta: 4 de junio de 2016).

OTROS DOCUMENTOS

ACCENTURE, "Always on. Always connected. Liderando la creación de un ecosistema digital sostenible", Estudio de 23 de julio de 2012, elaborado por Accenture y Ametic. Recuperado de:

http://www.accenture.com/es-es/Pages/always-on-always-connected-study-acn-ametic-2012.aspx (última consulta: 23 enero 2015).

ANTEPROYECTO DE CÓDIGO PROCESAL PENAL. Recuperado de: http://www.mjusticia.gob.es/cs/Satellite/es/1215198252237/ALegislativa_P/1288774452773/Detalle.html (última consulta: 12 febrero 2016).

ANTEPROYECTO DE LEY ENJUICIAMIENTO CRIMINAL. http://www.elderecho.com/actualidad/Anteproyecto-Ley-Enjuiciamiento-Criminal_EDEFIL20110728_0006.pdf (última consulta: 23 noviembre 2015).

ANTEPROYECTOS DE LEY INFORMADOS EN CONSEJOS DE MINISTROS. Recuperado de: http://www.mjusticia.gob.es/cs/Satellite/es/1215198252237/ALegislativa_P/1288774452773/Detalle.html (última consulta: 16 abril 2016).

BLACKBERRY MESSENGER. Recuperado de: http://appworld.blackberry.com/webstore/content/3729/?lang=es&countrycode=ES (última consulta: 23 abril 2014).

COMPAÑIA IRCOS JSC. Recuperado de: http://www.ircos.ru/es/ptb_d11pl.html (última consulta: 11 junio 2015).

FACEBOOK. Política de datos. Recuperado de: https://www.facebook.com/full_data_use_policy (última consulta: 22 de junio 2015).

GOOGLE. Política de privacidad. Recuperado de: http://www.google.com/intl/es_es/policies/privacy/ (última consulta: 2 abril 2015).

GOOGLE ALLO. Recuperado de: https://allo.google.com (última consulta: 23 mayo 2016).

GOOGLE HANGOUTS. Recuperado de: https://www.google.es/talk/intl/es/ (última consulta: 23 mayo 2016).

GROUPME. Recuperado de: https://groupme.com/ (última consulta: 12 junio 2016).

GRUPO NORT CONSULTING. Recuperado de: http://www.nortconsulting.net/new/nova.php?filId=9&filLin=es (última consulta: 22 enero 2015).

HEISE ONLINE. Recuperado de: http://www.heise.de/newsticker/meldung/Zoll-BKA-und-Verfassungsschutz-verschickten-2010-ueber-440-000-stille-SMS-1394593.html (última consulta: 13 marzo 2014).

IETF o The Internet Engineering Task Force. Recuperado de: http://www.ietf.org/ (última consulta: 9 junio de 2016)

IM+. Recuperado de: https://plus.im/ (última consulta: 11 julio 2016).

INCIBE. Recuperado de: http://www.inteco.es/ (última consulta: 15 septiembre 2015).

INSTAGRAM. Recuperado de: http://www.todoinstagram.com/3-aplicaciones-para-editar-la-localizacion-de-tus-fotos-de-instagram/ (última consulta: 10 junio 2013).

_____. Política de privacidad. Recuperado de: https://help.instagram.com/155833707900388 (última consulta: 10 junio 2013).

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. Recuperado de: https://www.ieee.org/index.html (última consulta: 17 julio 2013).

JOYN. Recuperado de: http://www.joynus.com/es/ (última consulta: 26 junio 2016).

LINE. Recuperado de: http://line.naver.jp/en/ (última consulta: 11 noviembre 2015).

NIMBUZZ MESSENGER. Recuperado de: http://www.nimbuzz.com/en/ (última consulta: 22 noviembre 2015).

PALTALK. Recuperado de: http://es.paltalk.com/ (última consulta: 7 febrero 2016).

PIDGIN. Recuperado de: http://www.pidgin.im/ (última consulta: 28 octubre 2016).

RADIOGONIOMETRÍA. Recuperado de: http://www.qsl.net/eb1hbk/taller/radiogonio.html (última consulta: 21 enero 2015).

_____.Recuperado de: http://www.uhistoria.com/uhistoria/tecnico/electronica/radiogoniometria/radiogoniometria.htm (última consulta: 23 febrero 2015).

SAMSUNG. ChatON. Recuperado de: http://www.samsung.com/es/article/que-es-chaton (última consulta: 12 mayo 2016).

SILENT SERVICES. Recuperado de: http://www.silentservices.de (última consulta: 2 febrero 2015).

SPOTBROS. Recuperado de: http://www.spotbros.com/ (última consulta: 6 noviembre 2015).

TANGO. Recuperado de: http://www.tango.me/ (última consulta: 2 mayo 2016).

TELEGRAM. Recuperado de: https://telegram.org (última consulta: 6 mayo 2015).

TUMe. Recuperado de: http://www.tu.com/es/me/ (última consulta: 22 diciembre 2014).

TWITTER. Política de datos. Recuperado de: https://about.twitter.com/es/what-is-twitter (última consulta: 30 septiembre 2014).

VIBER. Recuperado de: http://www.viber.com/ (última consulta: 4 mayo 2016)

VICUS. La Voz de Galicia. Recuperado de: http://www.lavozdegalicia.es/vigo/2010/11/18/00031290096441558452660.htm (última consulta: 30 octubre 2016)

_____.Faro de Vigo. Recuperado de: http://www.farodevigo.es/sociedad-cultura/2011/02/10/buscador-vicus-universidad-vigo-caza-65-pedofilos-cuatro-meses/517219.html_(última consulta: 30 octubre 2016)

WEB 2.0. Recuperado de: http://leonardoquinteros.blogspot.com.es/ (última consulta: 12 enero 2014).

WHATSAPP. Recuperado de: http://www.whatsapp.com/___(última consulta: 15 mayo 2015).

TEXTOS NORMATIVOS CONSULTADOS

Anteproyecto de la Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación.

Carta de los Derechos Fundamentales de la Unión Europea.

Código Penal.

Constitución Española.

Convenio Europeo de Derechos Humanos.

Convenio Internacional de Telecomunicaciones de Málaga-Torremolinos, ratificado por España el 29 de abril de 1976.

Convenio para la protección de los Derechos Humanos y de las Libertades Fundamentales, en Roma, 4 de noviembre de 1950.

Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

Convenio de asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, en Bruselas, 29 de mayo de 2000.

Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2001.

Decisión 676/2002/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, sobre un marco regulador de la política del espectro radioeléctrico en la Comunidad Europea.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

Directiva 2002/19/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión ("Directiva sobre acceso").

Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas ("Directiva sobre autorización").

Directiva 2002/21/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.

Directiva 2002/22/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas ("Directiva sobre servicio universal").

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas -*Directiva sobre la privacidad y las comunicaciones electrónicas*-, DOUE, núm. 201, de 31 de julio de 2002.

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, DOUE, núm. 105, de 13 de abril de 2006.

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, DOUE, núm. 105, de 13 de abril de 2006.

Directiva 2009/114/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, por la que se modifica la Directiva 87/372/CEE, de 25 de junio de 1987, relativa a las bandas de frecuencia a reservar para la introducción coordinada de comunicaciones móviles terrestres digitales, celulares públicas paneuropeas en la Comunidad.

Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) 2006/2004 sobre la cooperación en materia de protección de los consumidores.

Directiva 2009/140/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas.

Directiva 2012/27/UE, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, relativa a la eficiencia energética, por la que se modifican las Directivas 2007/127/CE y 2010/30/UE, y por la que se derogan las Directivas 2004/8/CE y 2006/32/CE.

Directiva 2014/41/CE del Parlamento Europeo y del Consejo, relativa a la orden europea de investigación en materia penal, DOUE, núm. 130, de 1 de mayo de 2014.

Ley Orgánica 7/1984, de 15 de octubre, sobre tipificación penal de la colocación ilegal de escuchas telefónicas.

Ley Orgánica 9/1984, de 26 de diciembre.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Ley de Enjuiciamiento Criminal.

Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Ley 9/2014, de 9 mayo, General de Telecomunicaciones.

Ley 25/2007, 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.

Orden ITC/110/2009, de 28 de enero, en relación a los requisitos y las especificaciones técnicas que resultan necesarios para el desarrollo del capítulo II del título V del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios aprobado por Real Decreto 424/2005, de 15 de abril. BOE núm. 29, de 3 de febrero de 2009.

Orden ITC/313/2010, de 12 de febrero, por la que se adopta la especificación técnica ETSI TS 101 671 "Interceptación legal (LI), Interfaz de traspaso para la interceptación legal del tráfico de telecomunicaciones". BOE núm. 43, de 18 de febrero de 2010.

Orden ITC/682/2010, de 9 de marzo, por la que se adopta la especificación técnica ETSI TS 133 108 (3GPP TS 33.108) "sistema de telecomunicaciones móviles universales (UMTS); LTE; seguridad 3G; interfaz de traspaso para la interceptación legal (LI)". BOE núm. 68, de 19 de marzo de 2010.

Orden IET/2530/2012, de 19 de noviembre, por la que se adoptan varias de las partes de la especificación técnica ETSI TS 102 232 «Interceptación Legal (IL); Interfaz de traspaso y detalles específicos de servicio (SSD) para la entrega mediante el protocolo IP». BOE núm. 285, de 27 de noviembre de 2012.

Real Decreto 863/2008, de 23 de mayo, por el que se aprueba el Reglamento de desarrollo de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico.

Real Decreto-Ley 13/2012, de 13 de marzo por el que se trasponen Directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajuste entre los costes y los ingresos de los sectores eléctrico y gasista.

Recomendación (2000)19 del Comité de Ministros del Consejo de Europa sobre el papel del Ministerio Fiscal en el sistema de justicia penal.

Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.

ANEXO. ÍNDICE CRONOLÓGICO DE JURISPRUDENCIA

I.- SENTENCIAS DEL TRIBUNAL SUPREMO

Sentencia del Tribunal Supremo, Sala 2ª, 298/1987, de 23 de enero,

Sentencia del Tribunal Supremo, Sala 2ª, 2271/1987, de 31 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 2852/1987, de 22 de abril,

Sentencia del Tribunal Supremo, Sala 2ª, 2867/1987, de 23 de abril,

Sentencia del Tribunal Supremo, Sala 2ª, 982/1988, de 16 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 3710/1998, de 17 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 6447/1988, de 23 de septiembre,

Sentencia del Tribunal Supremo, Sala 2ª, 7691/1988, de 3 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 12627/1989, de 5 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 9501/1991, de 21 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 10348/1993, de 26 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 4234/1993, de 18 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 4895/1993, de 2 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 7682/1993, de 15 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 135/1994, de 21 de enero,

Sentencia del Tribunal Supremo, Sala 2ª, 753/1994, de 11 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 1161/1994, de 23 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 5675/1994, de 22 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 18652/1994, de 17 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 8069/1994, de 12 de diciembre,

Sentencia del Tribunal Supremo, Sala 2ª, 198/1995, de 23 de enero,

Sentencia del Tribunal Supremo, Sala 2ª, 7285/1995, de 4 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 3997/1995, de 7 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 276/1996, de 2 de abril,

Sentencia del Tribunal Supremo, Sala 2ª, 738/1996, de 11 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 5496/1996, de 14 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 6013/1996, de 31 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 3672/1997, de 26 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 3806/1997, de 30 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 5113/1997, de 17 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 5884/1997, de 6 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 5997/1997, de 17 de diciembre,

Sentencia del Tribunal Supremo, Sala 2ª, 196/1998, de 19 de enero,

Sentencia del Tribunal Supremo, Sala 2ª, 6258/1998, de 27 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 6371/1998, de 31 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 6951/1998, de 23 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 1166/1999, de 20 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 1349/1999, de 27 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 2151/1999, de 24 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 373/1999, de 3 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 6133/1999, de 6 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 1521/1999, de 3 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 316/2000, de 3 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 123/2001, de 4 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 1235/2002, de 27 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, de 1647/2002, de 1 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 200/2003, de 15 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 498/2003, de 24 de abril,

Sentencia del Tribunal Supremo, Sala 2ª, 763/2003, de 30 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 1231/2003, de 25 de septiembre,

Sentencia del Tribunal Supremo, Sala 2ª, 1086/2003, de 25 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 1690/2003, de 15 de diciembre,

Sentencia del Tribunal Supremo, Sala 2ª, 9/2004, de 19 de enero,

Sentencia del Tribunal Supremo, Sala 2ª, 358/2004, de 16 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 182/2004, de 23 de abril,

Sentencia del Tribunal Supremo, Sala 2ª, 1075/2004, 24 de septiembre,

Sentencia del Tribunal Supremo, Sala 2ª, 2025/2004, de 6 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 129/2005, de 7 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 364/2005, de 28 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 705/2005, de 6 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 1090/2005, de 15 de septiembre,

Sentencia del Tribunal Supremo, Sala 2ª, 1222/2005, de 17 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 262/2005, de 24 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 1347/2005, de 16 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 1566/2005, de 30 de diciembre,

Sentencia del Tribunal Supremo, Sala 2ª, 324/2006, de 21 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 136/2006, de 8 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 706/2006, de 14 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 898/2006, de 16 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 1058/2006, de 2 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 343/2007, de 20 de abril,

Sentencia del Tribunal Supremo, Sala 2ª, 792/2007, de 30 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 562/2007, de 22 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 602/2007, de 4 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 662/2007, de 9 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 921/2007, de 6 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 25/2008, de 29 de enero,

Sentencia del Tribunal Supremo, Sala 2ª, 104/2008, de 4 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 236/2008, de 9 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 249/2008, de 20 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 292/2008, de 28 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 402/2008, de 30 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 104/2008, de 11 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 521/2008, de 24 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 25/2008, de 29 de agosto,

Sentencia del Tribunal Supremo, Sala 2ª, 776/2008, de 18 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 906/2008, de 19 de diciembre,

Sentencia del Tribunal Supremo, Sala 2ª, 940/2008, de 18 de diciembre,

Sentencia del Tribunal Supremo, Sala 2ª, 208/2009, de 6 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 250/2009, de 13 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 308/2009, de 23 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 548/2009, de 1 junio,

Sentencia del Tribunal Supremo, Sala 2ª, 704/2009, de 29 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 1078/2009, 5 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 1190/2009, de 3 diciembre,

Sentencia del Tribunal Supremo, Sala 2ª, 1315/2009, de 18 de diciembre,

Sentencia del Tribunal Supremo, Sala 2ª, 1215/2009, de 30 de diciembre,

Sentencia del Tribunal Supremo, Sala 2ª, 26/2010, de 27 de abril,

Sentencia del Tribunal Supremo, Sala 2ª, 27/2010, de 25 de enero,

Sentencia del Tribunal Supremo, Sala 2ª, 247/2010, de 18 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 327/2010, de 12 de abril,

Sentencia del Tribunal Supremo, Sala 2ª, 740/2010, de 6 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 680/2010, de 14 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 753/2010, de 19 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 764/2010, de 15 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 895/2010, de 14 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 79/2011, de 15 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 105/2011, de 23 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 185/2011, de 15 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 316/2011, de 6 de abril,

Sentencia del Tribunal Supremo, Sala 2ª, 286/2011, de 15 de abril,

Sentencia del Tribunal Supremo, Sala 2ª, 293/2011, de 14 de abril,

Sentencia del Tribunal Supremo, Sala 2ª, 565/2011, de 6 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 629/2011, de 23 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 1044/2011, de 11 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 15/2012, de 20 de enero,

Sentencia del Tribunal Supremo, Sala 2ª, 67/2012, de 9 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 109/2012, de 14 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 258/2012, de 30 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 410/2012, de 17 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 430/2012, de 29 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 478/2012, de 29 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 468/2012, de 11 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 554/2012, de 4 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 658/2012, de 13 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 676/2012, de 26 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 722/2012, de 2 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 740/2012, de 10 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 794/2012, de 11 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 777/2012, de 17 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 791/2012, de 18 de octubre,

Sentencia del Tribunal Supremo, Sala 2ª, 927/2012, de 27 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 241/2012, de 17 de diciembre,

Sentencia del Tribunal Supremo, Sala 2ª, 35/2013, de 18 de enero,

Sentencia del Tribunal Supremo, Sala 2ª, 143/2013, de 28 de febrero,

Sentencia del Tribunal Supremo, Sala 2ª, 209/2013, de 6 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 220/2013, de 21 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 649/2013, de 11 de junio,

Sentencia del Tribunal Supremo, Sala 2ª, 798/2013, de 5 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 849/2013, de 12 de noviembre,

Sentencia del Tribunal Supremo, Sala 2ª, 912/2013, de 4 de diciembre,

Sentencia del Tribunal Supremo, Sala 2ª, 587/2014, de 18 de julio,

Sentencia del Tribunal Supremo, Sala 2ª, 615/2014, de 25 de septiembre,

Sentencia del Tribunal Supremo, Sala 2ª, 167/2016, de 2 de marzo,

Sentencia del Tribunal Supremo, Sala 2ª, 426/2016, de 19 de mayo,

Sentencia del Tribunal Supremo, Sala 2ª, 841/2016, de 8 de noviembre.

II.- SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL

Sentencia del Tribunal Constitucional 11/1981, de 8 de abril,

Sentencia del Tribunal Constitucional 107/1983, de 29 de noviembre,

Sentencia del Tribunal Constitucional 114/1984, de 29 de septiembre,

Sentencia del Tribunal Constitucional 107/1985, de 7 de octubre,

Sentencia del Tribunal Constitucional 64/1986, de 21 de mayo,

Sentencia del Tribunal Constitucional 25/1988, de 23 de febrero,

Sentencia del Tribunal Constitucional 60/1988, de 8 de abril,

Sentencia del Tribunal Constitucional 137/1988, de 7 de julio,

Sentencia del Tribunal Constitucional 181/1989, de 3 de noviembre,

Sentencia del Tribunal Constitucional 201/1989, de 30 de noviembre,

Sentencia del Tribunal Constitucional 51/1990, de 26 de marzo,

Sentencia del Tribunal Constitucional 98/1990, de 20 de junio,

Sentencia del Tribunal Constitucional 154/1990, de 15 de octubre,

Sentencia del Tribunal Constitucional 41/1991, de 25 de febrero,

Sentencia del Tribunal Constitucional 80/1991, de 15 de abril,

Sentencia del Tribunal Constitucional 140/1991, de 20 de junio,

Sentencia del Tribunal Constitucional 138/1992, de 13 de octubre,

Sentencia del Tribunal Constitucional 303/1993, de 25 de octubre,

Sentencia del Tribunal Constitucional 323/1993, de 8 de noviembre,

Sentencia del Tribunal Constitucional 79/1994, de 14 de marzo,

Sentencia del Tribunal Constitucional 85/1994, de 14 de marzo,

Sentencia del Tribunal Constitucional 161/1999, de 27 de septiembre,

Sentencia del Tribunal Constitucional 51/1995, de 23 de febrero,

Sentencia del Tribunal Constitucional 86/1995, de 6 de Junio,

Sentencia del Tribunal Constitucional 100/1995, de 11 de junio,

Sentencia del Tribunal Constitucional 181/1995, de 11 de diciembre,

Sentencia del Tribunal Constitucional 200/1996, de 3 de diciembre,

Sentencia del Tribunal Constitucional 49/1996, de 26 de marzo,

Sentencia del Tribunal Constitucional 54/1996, de 26 de marzo,

Sentencia del Tribunal Constitucional 59/1996, de 15 de abril,

Sentencia del Tribunal Constitucional 248/1996, de 16 septiembre,

Sentencia del Tribunal Constitucional 40/1997, de 27 de febrero,

Sentencia del Tribunal Constitucional 153/1997, de 29 de septiembre,

Sentencia del Tribunal Constitucional 173/1997, de 14 de octubre,

Sentencia del Tribunal Constitucional 228/1997, de 16 de diciembre,

Sentencia del Tribunal Constitucional 81/1998, de 2 de abril,

Sentencia del Tribunal Constitucional 121/1998, de 15 de junio,

Sentencia del Tribunal Constitucional 151/1998, de 13 de julio,

Sentencia del Tribunal Constitucional 49/1999, de 5 de abril,

Sentencia del Tribunal Constitucional 166/1999, de 27 de septiembre,

Sentencia del Tribunal Constitucional 171/1999, de 27 de septiembre,

Sentencia del Tribunal Constitucional 236/1999, de 20 de diciembre,

Sentencia del Tribunal Constitucional 33/2000, de 14 de febrero,

Sentencia del Tribunal Constitucional 50/2000, de 28 de febrero,

Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre,

Sentencia del Tribunal Constitucional 299/2000, de 11 de diciembre,

Sentencia del Tribunal Constitucional 202/2001, de 15 de octubre,

Sentencia del Tribunal Constitucional 17/2001, de 29 de enero,

Sentencia del Tribunal Constitucional 138/2001, de 18 de junio,

Sentencia del Tribunal Constitucional 141/2001, de 18 de junio,

Sentencia del Tribunal Constitucional 28/2002, de 11 de febrero,

Sentencia del Tribunal Constitucional 70/2002, de 3 de abril,

Sentencia del Tribunal Constitucional 123/2002, de 20 de mayo,

Sentencia del Tribunal Constitucional 167/2002, de 18 de septiembre,

Sentencia del Tribunal Constitucional 188/2002, de 14 de octubre,

Sentencia del Tribunal Constitucional 205/2002, de 11 de noviembre,

Sentencia del Tribunal Constitucional 22/2003, 10 de febrero,

Sentencia del Tribunal Constitucional 184/2003, de 23 de octubre,

Sentencia del Tribunal Constitucional 165/2005, de 20 de junio,

Sentencia del Tribunal Constitucional 205/2005, de 18 de julio,

Sentencia del Tribunal Constitucional 259/2005, de 24 de octubre,

Sentencia del Tribunal Constitucional 261/2005, de 24 de octubre,

Sentencia del Tribunal Constitucional 26/2006, de 30 de enero,

Sentencia del Tribunal Constitucional 123/2006, de 24 de abril,

Sentencia del Tribunal Constitucional 253/2006, de 11 de septiembre,

Sentencia del Tribunal Constitucional 230/2007, de 5 de noviembre,

Sentencia del Tribunal Constitucional 66/2009, de 9 de marzo,

Sentencia del Tribunal Constitucional 197/2009, de 28 de septiembre,

Sentencia del Tribunal Constitucional 128/2011, de 18 de julio,

Sentencia del Tribunal Constitucional 173/2011, de 7 de noviembre,

Sentencia del Tribunal Constitucional 142/2012, de 2 de julio,

Sentencia del Tribunal Constitucional 241/2012, de 17 de diciembre.

III.- SENTENCIAS DE TRIBUNALES SUPERIORES DE JUSTICIA

STSJ Madrid 28/2010, de 25 de marzo, de declaración (caso Gürtel).

IV.- SENTENCIAS DE LA AUDIENCIA NACIONAL

Sentencia de la Audiencia Nacional, Sala de lo Penal, 65/2007, de 31 de octubre.

V.- SENTENCIAS DEL TRIBUNAL JUSTICIA DE LA UNIÓN EUROPEA

STJUE, de 10 de febrero de 2009,

STJUE, de 22 de noviembre de 2012,

STJUE, de 8 de abril de 2014.

VI.- SENTENCIAS DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS

STEDH de 2 de agosto de 1984, caso Malone *vs.* Reino Unido,

STEDH, Gran Sala, de 25 de junio de 1997, caso Halford *vs.* Reino Unido,

STEDH de 24 de agosto de 1998, caso Lambert *vs.* Francia,

STEDH de 15 de febrero de 2000, caso Amman *vs.* Suiza,

STEDH de 4 de mayo de 2000, caso Rotaru *vs.* Rumania,

STEDH de 20 de junio de 2000, caso Foxley *vs.* Reino Unido,

STEDH de 25 de septiembre de 2001, caso P.G. y J.H. *vs.* Reino Unido,

STEDH de 28 de enero de 2003, caso Peck *vs.* Reino Unido,

STEDH de 29 de marzo de 2005, caso Matheron *vs.* Francia,

STEDH de 3 de abril de 2007, caso Copland *vs.* Reino Unido,

STEDH de 16 de octubre de 2007, caso Wieser y Bicos Beiligungen GMBH *vs.* Austria,

STEDH de 22 de mayo de 2008, caso IlillaStefanov *vs.* Bulgaria,

STEDH de 1 de julio de 2008, caso Calmanovici *vs.* Rumania,

STEDH de 1 de julio de 2008, caso Liberty y otros *vs.* Reino Unido,

STEDH de 22 de diciembre de 2008, caso Aleksanyan *vs.* Rusia,

STEDH de 18 de mayo de 2010, caso Kennedy *vs.* Reino Unido,

STEDH de 2 de septiembre de 2010, caso Uzun *vs.* Alemania,

STEDH de 3 de julio de 2012, caso Robathin *vs.* Austria,

STEDH de 14 de marzo de 2013, caso BernhLarsenHoldingy otros *vs.* Noruega.

VII.- OTRAS SENTENCIAS DE CARÁCTER INTERNACIONAL

Sentencia del Tribunal Constitucional Alemán, de 2 de marzo de 2010,

Sentencia del Tribunal Supremo de EE.UU (Katz *vs.* United States, (1967),

Sentencia del Tribunal Supremo de EE.UU. (U.S. *vs.* Jones, (2012).