TRABAJO FIN DE GRADO

MONOGRÁFICO

BUENAS PRÁCTICAS EN LA LIMITACIÓN E INTROMISIÓN DE LOS DERECHOS FUNDAMENTALES

AUTOR: José Ignacio Almendral Pastor

TUTOR: Prof. Dr. Daniel Sanso Rubert Pascual

CONVOCATORIA: Ordinaria

GRADO EN DERECHO

Curso académico 2020/2021

FACULTAD DE CIENCIAS SOCIALES Y DE LA COMUNICACIÓN

UNIVERSIDAD EUROPEA DE MADRID

ABREVIATURAS

Sigla	Español	Inglés
ART	Art.	Article
BD	Disco Blue – ray	
BOE	Boletín Oficial del Estado	
CD	Disco Compacto	Compact disc
CE	Constitución Española	
DVD	Disco digital versátil	Digital Versatile Disc
EEUU	Estados Unidos	
FCS	Fuerzas y Cuerpos de Seguridad	European Convention Human Rights
FCSE	Fuerzas y Cuerpos de Seguridad del Estado	
GPS	Sistema de Posicionamiento Global	Global Positioning System
HDD	Disco Duro	Hard Disk Drive
LAJ	Letrado de la Administración de Justicia	
LECrim	Ley de Enjuiciamiento Criminal	
LO	Ley Orgánica	
RAE	Real Academia Española	Spanish Constitution
SSD	Disco solido	Solide State Drive
STC	Sentencia Tribunal Constitucional	
STEDH	Sentencia Tribunal europeo de derechos humanos	
STS	Sentencia Tribunal Supremo	
TC	Tribunal Constitucional	Code of Canon Law
TEDH	Tribunal Europeo de Derechos Humanos	
TS	Tribunal supremo	
UE	Unión Europea	
USB	Bus serie Universal	Universal Serial Bus

ÍNDICE

RESUMEN

El presente trabajo ha sido desarrollado con el objetivo de dar luz a las controversias creadas por parte de las FCS en los momentos de una solicitud de medidas restrictivas de algún derecho fundamental de la persona investigada ante instancias judiciales.

La restricción de una media así, siempre tomada por el Juez, como veremos en el presente trabajo, debe siempre cumplir unos parámetros que en muchas ocasiones no han sido del todo cumplidos, o que posteriormente el TS ha examinado más a fondo aún y ha detectado que en el recorrido del cumplimiento de todos los principios que debe cumplir, alguno de ellos se ha quedado sin un fundamento completo, lo que ha llevado en numerosas ocasiones a posteriores anulaciones de las medidas y con ello a desestimar unas medidas que han tumbado las investigaciones policiales.

Los nuevos avances tecnológicos han llevado a tener que actualizar nuestra LECrim, entrando de lleno en el art. 588 a través de la LO. 13/2015 de 5 de octubre de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de investigación tecnológica.

Esta ley introduce cambios jurídicos, sustantivos y procesales que a través de las sucesivas sentencias de los Tribunales se ha llegado a determinar os principios que se deben dar para la restricción de ciertas medidas limitativas de los derechos fundamentales a la hora de realizar las investigaciones policiales, determinándolos en el estricto cumplimiento de la especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad.

Palabras clave: Derechos fundamentales, geolocalización, grabación imagen y sonido, equipos informáticos y limitación de derechos

ABSTRACT

This paper has been developed with the aim of shedding light on the controversies created by the FCS at the time of a request for measures restricting a fundamental right of the person under investigation before the courts.

The restriction of such a measure, always taken by the judge, as we will see in this work, must always comply with certain parameters that on many occasions have not been fully complied with, or that the SC has subsequently examined in even greater depth and has detected that in the course of complying with all the principles that must be fulfilled, some of them have been left without a complete basis, which has led on numerous occasions to subsequent annulment of the measures and thus to the dismissal of measures that have overturned police investigations.

New technological advances have led to the need to update our LECrim, entering fully into art. 588 through the LO. 13/2015 of 5 October amending the Criminal Procedure Act to strengthen procedural guarantees and the regulation of technological research.

This law introduces legal, substantive and procedural changes that, through successive court rulings, have come to determine the principles that must be given for the restriction of certain measures limiting fundamental rights when carrying out police investigations, determining them in strict compliance with speciality, exceptionality, suitability, necessity and proportionality.

Keywords: Fundamental rights, geolocation, image and sound recording, computer equipment and limitation of rights.

1.INTRODUCCIÓN

1.1 Objeto del trabajo

El objetivo de esta investigación se centrará en la determinación de los principios que deben cumplir jurídicamente las FCSE en las motivaciones fundamentadas para la restricción de alguno de los derechos fundamentales.

1.2. Justificación

El presente trabajo doctrinal nace del debate abierto socialmente sobre la protección de los derechos fundamentales de la persona, así mismo la disyuntiva planteada ante la necesidad de protección de estos, más concretamente en los enfocados hacia la protección de los datos, que hace que se vulneren ciertos principios constitucionales en una injerencia leve propiciada por el propio autor y protector de los mismos.

Esto representa un especial interés relacionado con mi trabajo dentro de las FCSE, donde, en numerosas ocasiones, el arduo trabajo de investigación realizado por los miembros del Cuerpo, se han visto finalmente truncados por una mala praxis enfocada en la injerencia de ciertas limitaciones de derechos fundamentales, no así con el convencimiento sino con las oscuras opacidades escondidas en las leyes, lo que significa que debemos remitirnos a la jurisprudencia obtenida a través de las diferentes sentencias del TS y TC para adecuarnos a los principios rectores en su tramitación.

Con ello, se ha llegado a plantear cuestiones contrarias a las propias directrices doctrinales llegando a chocar, en ciertos puntos, entre la legislación nacional y la legislación madre del Tribunal de la Unión Europea, con repercusión directa en el ámbito nacional, teniendo siempre en cuenta la soberanía nacional que impera por encima de todo.

Por lo expuesto, tras conversaciones de ámbito penal nace la inquietud del análisis de la Directiva (UE) 2016/680[1] tras la STC de 31/01/2017 en referencia a la jurisprudencia del Tribunal Europeo de Justicia, destacando entre ellas la sentencia del asunto Van Duyn de 04/12/1974 o la más reciente del Asunto Ambisig del 07/07/2016 entre otras varias.

Dicha Directiva confronta directamente con lo legislado en la *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a la comunicaciones electrónicas y las redes*

[1] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos y por lo que se deroga la Decisión Marco 2008/977/JAI del consejo. BOEU de 4.5.2016

públicas de comunicación[2], donde en la citada Ley se determina un tiempo de conservación de datos generados por el dispositivo, que en numerosas ocasiones han dado inicio a muchas investigaciones en ámbito policial, por lo que a juzgar por la Directiva Europea, de posterior publicación, determina un plazo menor para el respaldo de los datos personales guardados, lo que pone en juicio de alerta a las numerosas investigaciones que se encuentran en instrucción, al dejar un vacío legal de protección jurídica de la cesión de datos. El debate nace en seno profesional, y aunque a día de hoy dicha directiva no se ha traspuesto a la legislación nacional, esta disyuntiva me hace plantear el presente trabajo, en búsqueda de determinar los parámetros adecuados y acordes a la jurisprudencia para una buena protección de las actuaciones en ámbito profesional.

En este sentido, analizando las nuevas tendencias tecnológicas y la armonización y modernización jurídica del tratamiento de datos personales, a fin de preservar un bien jurídico protegido legislativamente, es por lo que, partiendo esta primera idea se acabará analizando al detalle las nuevas formas de intromisión tecnológicas dentro del determinante art. 588 de la LECrim.

Teniendo una idea de inicio, a lo largo del desarrollo del citado trabajo se enfocarán los parámetros necesarios jurídicamente a través de la jurisdicción del Tribunal Supremo, de los principios necesarios para la correcta ejecución de la limitación de los derechos fundamentales, con una absoluta protección a los mismos y más concretamente enfocado en las medidas de la LO 13/2015, de 05 de octubre, de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas, centrándonos en el art. 588 de la vigente LECrim.

[2] Ley 25/2007, de 18 de octubre, de conservación de datos relativo a las comunicaciones electrónicas y a las redes públicas de comunicaciones. BOE núm. 251 §18243 (2007)

2. DESARROLLO DEL TRABAJO

Esta investigación se estructura en los puntos fundamentales y necesarios que deben conocerse desde la perspectiva del origen de una investigación para conseguir un esclarecimiento adecuado y ajustado legislativamente, teniendo muy presente el tipo de derecho fundamental, los requisitos necesarios, las fundamentaciones necesarias y el análisis de éste, para llegar a determinar el recorrido jurídico del derecho fundamental.

La premisa se estructurará en un trabajo monográfico de investigación, donde se analizará en profundidad las novedosas medidas legisladas 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 de la regulación de medidas de investigación tecnológicas,* y que han entrado de lleno a la reforma del art. 588 de la LECrim.

Sin llegar a tocar todos y cada uno de los Derechos Fundamentales recogidos constitucionalmente, se ha visto de interés el estudio de la geolocalización realizada de las personas en la era tecnológica, que entra de lleno en el punto del consentimiento. Además se ha visto conveniente hilarlo con los procedimientos de las grabaciones de imágenes y sonidos, para terminar con las intromisiones permitidas en los aparatos electrónicos utilizados por las personas.

2.1 Conceptos de Fuentes Fundamentales

La RAE, define los derechos fundamentales "*los derechos declarados por la Constitución que gozan del máximo nivel de protección*", por lo que se liga directamente a unos derechos inalienables, inviolables e irrenunciables. Por ello pertenecen indudablemente a todas las personas por el simple hecho de existencia, o lo que podemos determinar de otra forma, por el simple hecho de ser persona, que con ello es otro derecho más.

Nuestra Carta Magna en su Título I. De los derechos y deberes fundamentales, determinado con su art. 10[3] el reconocimiento de la dignidad humana, recogido en nuestro

[3] **Art. 10**
1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.
2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

ordenamiento jurídico de acorde a los principios la Declaración Universal de los Derechos Humanos y todos aquellos tratados y acuerdos internacionales que España ha ratificado.

En este sentido, hay que diferenciar la catalogación de los derechos fundamentales, frente a los derechos humanos, entendiendo estos últimos, como aquellos que no encuentran obstáculo ante un límite territorial, económico, social o personal, siendo de todo modo Universales, Inviolables, Intransferibles, Irrenunciables e Interdependientes.

En relación con los derechos enumerados, hoy en día, nuestra sociedad tiende cada vez más a borrar la línea que separa los derechos de los deberes. La ética social, cada vez menos valorada, hacen que, tanto desde la perspectiva de la persona entendamos ciertas atribuciones que no nos pertenecen como persona, a atribuirlas como derecho inherentes a la misma, de igual forma que, inconscientemente dejamos que los poderes públicos se entrometan directamente en todo aquello que deberían de defender y proteger de cara al ser humano, llegando a confundirlo como obligación desde el punto de vista de la persona, cuando realmente es un derecho del ciudadano y un deber de los poderes públicos.

Teniendo en cuenta estas connotaciones éticas, donde pudiera crearse una laguna jurídica sin llegar a regular, y donde de facto se han ido realizando injerencias en los derechos fundamentales de las personas que posteriormente necesitarían del apoyo jurisdiccional de los propios magistrados, y de las diversas modificaciones a través de las diversas sentencias del Tribunal Supremo, con el fin de determinar un equilibrio se introduce en nuestro ordenamiento jurídico 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 de la regulación de medidas de investigación tecnológicas*[4].

Con la introducción de las modificaciones ejercidas en la LECrim, a través de este nueva ley, donde nuestro Código Procesal, como bien dice en su preámbulo "*plantea un cambio radical del sistema de justicia penal",* consigue dotar aún más nuestro ordenamiento jurídico de un carácter garantista, de acorde a las exigencias marcadas por el Derecho de la Unión Europea, dando mayor fortalecimiento y dotando la restricción de derechos fundamentales, en cuanto a los de investigación tecnológica enfocados al ámbito de la intimidad, el secreto de las comunicaciones, de una serie de restricciones y principios que

[4] 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 §10725 (2015)

se deben cumplir por parte de las FCS, a la hora de realizar las solicitudes judiciales para que sean motivadas dichas restricciones.

Ya la propia Ley determina los principios que se deben regir en cuanto a la restricción de ciertos derechos fundamentales, marcados por el alto TC donde define que toda medida de injerencia debe respetar el principio de especialidad, es decir que se investiguen hechos concretos. A este respecto, el propio preámbulo 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 de la regulación de medidas de investigación tecnológicas* determina la prohibición de todas aquellas medidas de investigaciones prospectivas, entendiendo estas como todas aquellas que se inician buscando el delito, o mejor dicho «*No se puede salir a investigar 'en modo a ver lo que pesco'. Está proscrito y, además, es ilegal*», como expuso Alejandro Abascal, magistrado juez de refuerzo del Juzgado Central de Instrucción 6 de la Audiencia Nacional en el marco de la jornada «El secreto de sumario y la libertad de prensa: Los juicios paralelos[5]»

Además del principio de especialidad, todas aquellas medidas de carácter tecnológico deben responder al principio de idoneidad, entendiendo esta como la relación de causalidad, de medio a fin entre el medio adoptado y el fin medio a fin, entre el medio adoptado y el fin propuesto. Es decir, se trata del análisis de una relación medio-fin.

El Alto Tribunal marca también la necesidad del cumplimiento en todas las investigaciones tecnológicas del principio de excepcionalidad, entendiendo este como toda protección a esos derechos fundamentales inherentes y especiales de la persona para que las medidas tomadas en las investigaciones no sean otras que las que resulten menos gravosas hacia la persona.

Otro principio que debe reunir cuando hablamos de injerir en un derecho fundamental en todas las investigaciones tecnologías es el principio de necesidad y proporcionalidad, entendiendo estas como la necesidad de la existencia de una investigación previa que ayude a esclarecer la investigación, resultando esta como la única forma legal de poder llegar al esclarecimiento del delito (STS 141/2020, de 13 de mayo[6]) y el principio de

[5] Confilegal. *2020 Las investigaciones prospectivas "a ver lo que pesco" están prohibidas en nuestro ordenamiento jurídico*, Recuperado de https://confilegal.com/20190428-las-investigaciones-prospectivas-a-ver-lo-que-pesco-estan-prohibidas-en-nuestro-ordenamiento-juridico/

[6] STS, *Manuel Marche Gómez. España* de 13 de mayo de 2020

proporcionalidad como la determinación de la medida adecuada con la menor injerencia lesiva al derecho fundamental atacado, de tal forma que en muchas ocasiones, con la ejecución desmesurada de la proporcionalidad se está rebajando el hecho lesivo.

Dentro de todas las medidas que se determina 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 de la regulación de medidas de investigación tecnológicas* el presente trabajo se centrará en el análisis jurisdiccional de lo centrado en el Titulo VIII del Libro II con la redacción de su nuevo Capítulo IV que se rubrica "*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"*

Entre las medidas determinadas en el Capítulo, este trabajo se centrará en varios de ellos, con un análisis jurisdiccional de los mismo, con el objetivo de la determinación exhaustiva de los cumplimientos necesarios para que la intromisión en los derechos fundamentales de la persona, en este caso en la persona investigada, sea de la menor lesividad posible y ajustado a derecho, con el fin último de dotar a las Fuerzas y Cuerpos de Seguridad de las garantías procesales que determinan sus actuaciones.

Dentro de las modificaciones tomadas en el Titulo VIII del Libro II, con la narración del nuevo Capítulo IV, y refiriéndose a la "*utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes"*, se pueden determinar una serie de medias novedosas algunas de ellas como puede ser el uso de drones por parte de las FCS para la vigilancia de la seguridad pública, o medias no tan novedosas como las ya utilizadas balizas de geoposicionamiento.

Con el fin de vislumbrar un horizonte de seguridad jurídica en las actuaciones de las FCS en uso de las atribuciones realizadas para la prevención, investigación, detección o el enjuiciamiento de las infracciones penales, y sin dejar en olvido el resto de las limitaciones realizadas en el art. 588 de la LECrim, se comenzará con el análisis de la geolocalización como medida restrictiva en la investigación.

2.2. EL USO DE LA GEOLOCALIZACIÓN

Como regulan los apartados 1 y 2 del art. 588.quiquies. b de la LECrim, la autorización del juez deberá acreditar que haya razones de necesidad para la utilización de la medida, y que esta resulte proporcionada, debiendo especificar el medio técnico que va a ser utilizado, de manera que no será necesario identificar a los presuntos autores de los delitos que se van a investigar, sino solo el objeto sobre el que se colocará el dispositivo.

Antes de que la Ley Orgánica 13/2015, de 5 de octubre entrara en vigor, la policía judicial estaba habilitada para colocar una baliza sin autorización judicial, ya que no se observaba una vulneración en el secreto de comunicaciones, y la incidencia sobre el derecho a la intimidad era prácticamente nula. Esta técnica policial hoy en día únicamente requiere de la colocación de un pequeño dispositivo, que delata en todo momento la posición del investigado por medio de la recepción de datos de posicionamiento GPS. Al delatar su posición, permite el seguimiento a distancia desde un monitor que contenga la cartografía adecuada para situar la señal GPS en un mapa, estando limitado solamente por la batería que alimente el dispositivo oculto.

En la actualidad se utilizan este tipo de dispositivos para un abanico muy variado de situaciones que van desde la navegación por motivos de seguridad, los sistemas antirrobo del coche o para fines científicos, como pueden ser el estudio de los movimiento y migraciones de numerosas clases de animales. Si la baliza proporciona información de la persona las 24 horas, estamos obteniendo información precisa acerca de sus hábitos, comportamientos, relaciones y actividades.

La doctrina en esta materia, anterior a la entrada en vigor de la Ley Orgánica 13/2015, la encontramos en la sentencia del TS 562/2007, de 22 de junio[7], en donde dice que el artificio colocado permitió el seguimiento por mar de una embarcación sobre la que recaían sospechas de tráfico de droga**.** *Para su colocación en el exterior del barco no se precisó ninguna injerencia en ámbitos de intimidad constitucionalmente protegidos, por lo que la diligencia de investigación es legítima.*

El cambio de criterio que realiza la Ley Orgánica 13/2015 tiene una marcada tendencia garantista, ya que lo cierto es que la colocación del GPS es una diligencia legítima, que no necesita de autorización ya que no afecta a un derecho fundamental, sobre todo porque la baliza se adhiere al exterior de ciertos objetos (como puede ser un barco, un coche, un

[7] STS, *Andrés Martínez Arrieta. España* de 22 de junio de 2007

contenedor, etc..). En esto debió influir la sentencia del Tribunal Europeo de Derechos Humanos de 2 de septiembre de 2010 (Uzun c. Alemania) que señaló que la obtención de datos vía GPS constituyó una interferencia en la vida privada del apelante, pero esta intromisión estaba justificada al haber indicios de la comisión de un delito grave.

Como regulan los apartados 1 y 2 del art. 588.quiquies. b de la LECrim, la autorización del juez deberá acreditar que haya razones de necesidad para la utilización de la medida, y que esta resulte proporcionada, debiendo especificar el medio técnico que va a ser utilizado, de manera que no será necesario identificar a los presuntos autores de los delitos que se van a investigar, sino solo el objeto sobre el que se colocará el dispositivo.

Volviendo con la sentencia del caso Uzun tratada anteriormente, nos encontramos con que emplea el término **"***expectativa razonable de privacidad***",** que es un término que ya fue utilizado en otras sentencias anteriores como la del Caso Katz (STEDH de 20 de enero de 2009 Katz c. Rumania). Este término se utiliza para indicar que la sistemática recopilación y almacenamiento de datos por los servicios de seguridad respecto de particulares constituye en sí una interferencia en el derecho a la vida privada de los particulares, incluso sin el uso o cobertura de métodos de vigilancia.

Este concepto lo extrapola a la jurisprudencia norteamericana la sentencia del TS 610/2016, de 7 de julio de 2016[8], que nos dice que el caso EEUU v. Jones trata de dar una respuesta coherente a la grave injerencia sobre la privacidad de una persona que es sometida a una vigilancia discreta, prolongada incluso más allá de los límites de una autorización judicial expresa, vigilancia que se da por medio de un dispositivo de localización escondido en los bajos de un turismo. El derecho que tienen los ciudadanos a no verse sometidos a irrazonables registros o incautaciones en sus personas, domicilios, papeles o efectos, convierte a unos y otros en una especie de esferas de protección ad intra, pero encuentra una frontera difícil de superar cuando los supuestos actos de intromisión respetan el contenido al incidir extramuros de sus contornos físicos. De esto podemos extraer que debe de haber un acceso o contacto físico con algún objeto propiedad de la persona ofendida.

En cuanto a los delitos que pueden ser objeto de la utilización de dispositivos de seguimiento y localización nos encontramos con que no están regulados en el Capítulo VII, por lo que debemos atender a las disposiciones comunes que aparecen reguladas en

[8] STS, *Carlos Granados Pérez. España* de 7 de julio de 2016

el Capítulo IV. Dentro de este capítulo tenemos que prestar atención a los principios rectores, sobre todo a los principios de especialidad, que habla de un delito concreto, y de proporcionalidad que se refiere a la gravedad del hecho. La gravedad del hecho a la que se refiere el principio de proporcionalidad no es en función de la pena eventualmente aplicable, sino que hace referencia a la propia naturaleza de los hechos, a su mecánica de comisión, y a las inevitables necesidades para su ulterior probanza, por ello su autorización judicial deberá estar especialmente motivada.

Por todo lo visto en este punto podemos concluir que la colocación de cualquier dispositivo o medio técnico de geolocalización que tenga relación ya sea directa o indirecta, con una persona exige una autorización judicial amparándose en el derecho a la intimidad. En caso de que no se vea afectado el derecho a la intimidad (por colocar los mecanismos de control en contenedores, por ejemplo) no será necesaria la autorización judicial.

1. Medios de seguimiento y localización

Con la LO 13/2015 se introdujeron cambios legislativos al respecto de las medidas de investigación tecnológicas, entre las que se encuentran los medios o dispositivos de seguimiento y localización. Estos suponen una limitación al derecho a la intimidad del investigado (art. 18.1 CE), puesto que aportan datos de la posición de movimiento del investigado y facilitan su localización.

Estos medios son las denominadas “balizas”, dispositivos GPS o similar, controlados por la Policía Judicial, que se instalan en un vehículo o cualquier otro objeto que pudiera llevar consigo el investigado, permitiendo vigilar sus desplazamientos.

2. Requisitos Colocación

En la reforma de la Ley de Enjuiciamiento Criminal de 2015 se introduce la necesidad de autorización judicial para la colocación y utilización de dispositivos de seguimiento y localización, con excepciones de urgencia, a diferencia de la anterior regulación, que no la exigía (STS 610/2016, de 7 de julio).

2.1. Solicitud de autorización judicial.

La solicitud de colocación de la baliza al juez se debe hacer mediante oficio policial, que debe contener:

1. La **descripción del hecho objeto de investigación** y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.

2. La **exposición detallada de las razones que justifiquen la necesidad de la medida** de acuerdo con los principios rectores, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación "*suficiente investigación previa que aporte indicios que justifiquen la medida*" (STS 7-7-2016 en referencia a reiterada jurisprudencia).

Se rebajan las exigencias necesarias para la utilización de esta técnica de investigación en relación con otras ya que reiterada jurisprudencia ha determinado que supone una menor intromisión en los derechos fundamentales (STS 7-7-2016, TEDH), pero de igual modo deben de justificarse los siguientes principios:

- **Necesidad**: que exista una investigación previa que ponga de manifiesto que el uso de esta medida contribuye a avanzar en el descubrimiento de los comportamientos delictivos que se investigan. Para ello se deben aportar datos e indicios concretos y objetivos. EJ: *notitia criminis* (confidencia anónima) seguida de labores policiales de comprobación suficientes que aporten determinados indicios objetivos que hagan necesaria la colocación del dispositivo para la buena marcha de la investigación (STS 141/2020, de 13 de mayo[9]).

- **Especialidad**: que la medida se utilice para la investigación de un delito concreto

- **Idoneidad**: que sea adecuada respecto de la persona y delito investigado y durante el tiempo imprescindible

- **Excepcionalidad**: que no sea posible el recurso a otras técnicas de investigación que resulten menos gravosas que ésta para los derechos fundamentales

- **Proporcionalidad**: que se lleve a cabo un juicio de ponderación entre los beneficios para la investigación que se pueden conseguir con esta medida sean superiores a la limitación del derecho a la intimidad que con ella se produce. Como supone una menor injerencia que otras medidas, este juicio de proporcionalidad no debe ser tan estricto, pudiendo rebajar la gravedad del delito investigado

[9] STS, *Manuel Marchena Gómez. España*. de 13 de mayo de 2020.

FALTA DE MOTIVACIÓN: "*No podemos aceptar como norma general que esos tres elementos indiciarios (a) una confidencia anónima en la que se decía que el acusado, con domicilio en Villagarcía de Arosa estaba realizando viajes desde esa localidad a Ponferrada (León), transportando cocaína para ser suministrada a varias personas; b) la existencia de antecedentes policiales por delito de tráfico de drogas en la base policial del Ministerio del Interior; c) la constatación, a través del sistema de cámaras de la Dirección General del Tráfico, de que el acusado se desplazaba desde Villagarcía de Arosa a Ponferrada) sean suficientes para arrebatar a cualquier ciudadano el inicial blindaje que le proporciona su derecho a la intimidad. Una confidencia anónima, sin más, que no ofrezca otros elementos de corroboración que los antecedentes policiales y la realidad de unos viajes, no debería haber llevado a respaldar una resolución judicial habilitante para la restricción de derechos* (STS 141/2020 de 13 de mayo)

3. 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. Es preceptiva la **especificación del medio técnico que vaya a ser utilizado** para valorar el juicio de proporcionalidad**.**

4. La extensión de la medida con especificación de su contenido

5. La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.

6. La forma de ejecución de la medida.

7. La duración de la medida que se solicita.

8. El sujeto obligado que llevará a cabo la medida, en caso de conocerse.

Por ello no podemos dejar de obviar lo determinado jurídicamente en la STS610/2016 de 7 de julio de 2016[10], donde se deja claro los requisitos necesarios para la toma de medidas restrictivas de este calado, en su literal "*el respeto de los principios de previa habilitación normativa y superación de los juicios de proporcionalidad en sentido amplio, y de idoneidad, necesidad y proporcionalidad en sentido estricto, como nos recuerda, ad exemplum, la STC 123/2002, de 20 de mayo*[11] *, cuando proclama que: "... para*

[10] STS, *Carlos Granados Pérez. España* de 7 de julio de 2016

[11] STC *Manuel Jiménez de Parga y Cabrera, Pablo García Manzano, Fernando Garrido Falla, María Emilia Casas Baamonde y Javier Delgado Barrio, España* de 20 de mayo de 2002

comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad es necesario constatar si cumple estos tres requisitos: a) si la medida acordada puede conseguir el objetivo propuesto (juicio de idoneidad); b) si es necesaria en el sentido de que no exista otro medio más moderado para conseguir el fin propuesto con igual eficacia (juicio de necesidad); c) si la medida es ponderada o equilibrada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"

2.2. Casos de urgencia

Excepcionalmente se admite que la Policía Judicial instale un dispositivo GPS sin previa habilitación judicial cuando se den tres requisitos sin los cuales se puede generar la nulidad de los datos obtenidos por el dispositivo (SSTC no 281/2006, de 9 de octubre, entre otras):

- **Razones de urgencia**: casos en los que se disponga de un plazo de tiempo para la colocación del dispositivo que no permita acudir a la autoridad judicial para solicitar la autorización (STS 610/2016 de 7 de julio; STS nº 1025/2013
- **Situación de necesidad**: que esa situación de urgencia haga temer razonablemente que, de no colocarse inmediatamente el dispositivo, pudiera frustrarse la investigación, resultando absolutamente imprescindible la colocación para el éxito de la investigación
- **Que la Policía Judicial dé cuenta al Juez** con la mayor brevedad posible y, en todo caso, en el plazo máximo de veinticuatro horas, y que el Juez competente ratifique la medida. Para acreditar el cumplimiento de los plazos resulta aconsejable que se haga constar en el oficio policial que se presente ante el Juez la hora exacta tanto de la instalación del dispositivo como de la presentación del oficio en el Juzgado.

Pero se determina de forma clara en la referida sentencia del Tribunal Constitucional 281/2006, de 9 de octubre[12] en su literal "*La Convención de Naciones Unidas contra el tráfico ilícito de estupefacientes y sustancias psicotrópicas, hecha en Viena en 1988, prevé en su art. 7.9 que las solicitudes se presentarán por escrito si bien por razones*

[12] STC *María Emilia Casas Baamonde, Javier Delgado Barrio, Roberto García-Calvo y Montiel, Jorge Rodríguez-Zapata Pérez, Manuel Aragón Reyes y Pablo Pérez Tremps. España* de 9 de octubre de 2006

de urgencia pueden efectuarse verbalmente, debiendo ser confirmadas seguidamente por escrito. En las solicitudes de asistencia judicial deberá figurar entre otros datos —art. 7.10— "a) La identidad de la autoridad que haga la solicitud; b) El objeto y la índole de la investigación, del proceso o de las actuaciones a que se refiera la solicitud y el nombre y funciones de la autoridad que esté efectuando dicha investigación, dicho procesamiento o dichas actuaciones; c) Un resumen de los datos pertinentes ... d) Una descripción de la asistencia solicitada y de los pormenores". Igualmente en el Convenio europeo de asistencia judicial en materia penal —Estrasburgo 1959, ratificación en BOE núm. 223, de 17 de septiembre de 1982—, prevé en su art. 14 que las solicitudes de asistencia judicial deberán contener "a) autoridad que formula la solicitud, b) objeto y motivo de la solicitud, c) en lo posible, identidad y nacionalidad de la persona de que se trate, y d) nombre y dirección del destinatario, cuando proceda". En el Segundo Protocolo adicional a dicho Convenio —Estrasburgo, 8 de noviembre de 2001—, aún no ratificado por España, en su art. 4 que modifica el art. 15 del citado Convenio, establece que las solicitudes se harán por escrito, si bien precisa en su número noveno que "las solicitudes de asistencia judicial o cualquier otra comunicación en virtud del presente Convenio o de sus protocolos, pueden ser realizadas por conducto de medios electrónicos de comunicación, o por cualquier otro medio de telecomunicación, a condición de que la parte requirente esté en disposición de producir en todo momento, a solicitud de la otra parte, una copia escrita de lo expedido así como el original."

3. Duración y control de la medida:

La colocación del dispositivo GPS tiene un plazo inicial de duración de **tres meses** con la posibilidad de su **prórroga por el mismo o inferior plazo, hasta un máximo de duración de dieciocho meses, de forma excepcional**. Cuanto más tiempo se solicite el mantenimiento de la medida, mayor deberá ser el juicio de proporcionalidad, ya que se incrementa la intromisión en la intimidad del investigado.

El cómputo del tiempo comienza en la fecha de la resolución judicial que autorice la medida y no en el momento de la concreta colocación del dispositivo técnico.

Por otra parte, la Policía Judicial tiene obligación de informar al Juez de Instrucción del desarrollo y los resultados de la medida, así como de entregarle los soportes originales o copias electrónicas que contengan la información recogida, en la forma y con la

periodicidad que éste determine y, en todo caso, cuando por cualquier causa se ponga fin a la investigación.

4. Cese de la medida:

El cese de la medida se producirá cuando se cumpla cualquiera de los siguientes motivos:

- la desaparición de las circunstancias que justificaron su adopción
- que se evidencie que con la medida no se obtienen los resultados pretendidos
- que haya transcurrido el plazo inicialmente fijado para su ejecución

2.3 EL USO DE LAS GRABACIONES DE IMAGEN Y SONIDO

La grabación de imágenes y comunicaciones orales (sonido) del investigado se diferencia en su regulación.

1. Grabación de imágenes:

1.1. Según el lugar al que afecte la grabación:

A) En lugares públicos:

Existen varías garantías legislativas por las que las FCSE pueden acceder o captar grabaciones:

a) Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal[13], en adelante LECrim (investigación):

El art. 588 quinquies a autoriza a captar (lo que se puede denominar ver en tiempo real) y grabar imágenes (grabación almacenada que se perpetúa en el tiempo) a cualquier persona investigada[14] cuando se encuentre en un lugar o espacio público. Cuando se habla de *lugares o espacios públicos,* deberá interpretarse que se incluyen aquellos en los que el investigado no pueda ejercer su derecho a la intimidad, donde no pueda reservar al conocimiento de los demás lo que está sucediendo al no disponer de ningún derecho de exclusión sobre ese lugar, (ejemplo de lugar público sería un club de campo privado; al contrario, un ejemplo de lugar privado sería el vestuario del gimnasio o baño público de ese club de campo, donde la persona puede limitar el acceso a terceros). Debe entenderse como lugar público todo aquel que no constituya domicilio de una persona determinado como domicilio lo acentuado en la STS 731/2013, de 7 de octubre[15] que define en su literal "*el Tribunal Constitucional, ha identificado el domicilio con un 'espacio apto para desarrollar vida privada' (STC 94/1999, 31 de mayo, F. 4)[16], un espacio que 'entraña*

[13] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. BOE núm. 260 §6036 (1882)

[14] La propia 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 tecnológicas, adecua los términos utilizados hasta el momento a un lenguaje procesal de acorde a los tiempos en los que vivimos, y evitar así las connotaciones discriminatorias de la propia Ley al determinar "imputado" cuando no existe ningún tipo de sospecha ni evidencia, por lo que la propia Comisión para la claridad del Lenguaje Jurídico, actualizas los vocablos de imputado por investigado o encausado, haciendo una diferencia entre los mismo según el momento procesal en el que se encuentren, siendo el investigado toda aquella persona que se encuentra investigada por la relación con un delito y encausado la persona que ha sido imputada judicialmente.

[15] STS, *Manuel Marchena Gómez, España* de 7 de octubre de 2013

[16] STC, Carles Viver Pi-Sunyer, Rafael de Mendizábal Allende, Julio González Campos, tomas Salvador vives Antón, Vicente Conde Martin de Hijas y Guillermo Jiménez Sánchez, España de 31 de mayo de 1999.

una estrecha vinculación con su ámbito de intimidad', 'el reducto último de su intimidad personal y familiar' (STC 22/1984, STC 60/1991 y 50/1995, STC 69/1999, 26 de abril y STC núm. 283/2000, 27 de noviembre).

Esta Sala, entre otras en la STS 1108/1999, 6 de septiembre, ha afirmado que 'el domicilio es el lugar cerrado, legítimamente ocupado, en el que transcurre la vida privada, individual o familiar, aunque la ocupación sea temporal o accidental' (SSTS 24-10-1992, 19-7-1993 y 11-7-1996). Se resalta de esta forma la vinculación del concepto de domicilio con la protección de esferas de privacidad del individuo, lo que conduce a ampliar el concepto jurídico civil o administrativo de la morada para construir el de domicilio desde la óptica constitucional, como instrumento de protección de la privacidad"

Cámaras de vigilancia en lugares de acceso público, aunque este acceso sea restringido, ejemplo STS 28-1-2014[17]: "*el material fotográfico y videográfico obtenido en el ámbito público y sin intromisión indebida en la intimidad personal o familiar tiene un valor probatorio innegable." "la captación de imágenes de actividades que pueden ser constitutivas de acciones delictivas se encuentra autorizada por la ley en el curso de una investigación criminal, siempre que se limiten a la grabación de lo que ocurre en espacios públicos fuera del recinto inviolable del domicilio o de lugares específicos donde tiene lugar el ejercicio de la intimidad*."

Ejemplo STS 5-6-2013[18]: "*legitimidad de la grabación al ser realizada en un lugar - espacio público con acceso restringido- en el cual en el que no se desarrollan actividades propias de la intimidad de las personas." "la sala de atestados de las dependencias de la Policía Municipal de Alcorcón No es un espacio, efectivamente, equiparable a "aquellos medios de captación de la imagen o del sonido que filmaran escenas en el interior del domicilio prevaliéndose de los adelantos y posibilidades técnicas de estos aparatos grabadores, aun cuando la captación tuviera lugar desde emplazamientos alejados del recinto domiciliario, ni tampoco puede autorizarse la instalación de cámaras en lugares destinados a actividades donde se requiere la intimidad como las zonas de aseo*."

[17] STS, *Milagros Calvo Ibarlucea*. *España* de 28 de enero de 2014
[18] STS, *María Lourdes Arastey Sahun, España* de 5 de junio de 2013

Con esta medida, no se produce afectación a ninguno de los derechos fundamentales del art. 18 de nuestro texto constitucional. De ahí que resulte innecesaria la autorización judicial para su utilización por la Policía Judicial.

"*Lo relevante es discernir cuando se trata de un espacio reservado a la autorización judicial, domicilio o lugar cerrado, o cuando por propia iniciativa los agentes pueden captar las imágenes cuestionadas por tratarse de "lugares o espacios públicos", pues en estos, incluyendo con carácter general todos aquellos ajenos a la protección constitucional dispensada por el art. 18.2 de la Constitución Española a la inviolabilidad domiciliaria o por el art. 18.1 a la intimidad, podrá ser decidida por propia iniciativa por los agentes de policía*" (STS nº 272/2017[19], de 18 de abril).

Lo que determinará, por lo tanto, la necesidad de autorización judicial será la afectación de algún derecho fundamental (inviolabilidad domiciliaria, intimidad, secreto de las comunicaciones o protección de datos), quedando limitado el ámbito de aplicación de la medida por simple iniciativa policial al resto de los supuestos.

El criterio que va a determinar cuándo se afecta o no el derecho fundamental no va a ser el lugar donde se coloque el dispositivo de captación de la imagen (público o privado), sino el lugar o espacio público o privado donde se encuentre el sujeto objeto de la grabación.

b) Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos[20].

Por la que se regula la utilización de videocámaras por las FCS en lugares públicos, que permite en su art. 1 la utilización por las FCS de videocámaras para grabar imágenes y sonidos en lugares públicos.

Se exige la existencia de un riesgo razonable para la seguridad pública en el caso de instalación de cámaras fijas, y de un peligro concreto para el uso de las móviles, conforme a las exigencias del principio de proporcionalidad. Ambas se regulan por una tramitación administrativa.

[19] STS *Juan Saavedra Ruiz, España* de 18 de abril de 2017
[20] Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. BOE núm. 186 §17574 (1997)

En caso de que se capten hechos que podrían ser constitutivos de delito, las FCS pondrán la cinta o soporte original de las imágenes y sonidos en su integridad a disposición judicial con la **mayor inmediatez posible** y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación. Esta es una de las circunstancias más importantes, para evitar su posible manipulación.

"S*e hace rigurosamente necesario activar las medidas de control judicial oportunas para evitar alteraciones, trucajes o montajes fraudulentos o simples confusiones, es decir, para garantizar la autenticidad del material videográfico, lo que, a su vez, requiere la inmediata entrega a la autoridad judicial del original de la grabación*" (STS nº 200/2017[21], de 27 de marzo y STS 10-3-2020[22])

"*No puede alegarse una desproporción en el uso del contenido de las imágenes obtenidas en las cámaras de grabación instaladas con arreglo a la protección de datos y a la regulación específica en la materia, y, como se ha expuesto, por razones de prevención del delito."" en el proceso penal se ha obtenido con el tratamiento de los datos realizados a instancia de las fuerzas y cuerpos de seguridad del Estado en una cámara de grabación instalada con arreglo a la Ley de protección de datos. Precisamente, el tratamiento de sus datos es legítimo y correcto su uso adecuado por parte por parte de las fuerzas y cuerpos de seguridad del Estado y, en consecuencia, ello no provoca una injerencia en el derecho"* (STS 10-3-2020).

c) Ley 5/2014, de 4 de abril, de Seguridad Privada[23].

Aquí, las diferencias son mayores, ya que la grabación no se realiza por las FCSE y no se captan imágenes que tengan lugar en espacios públicos; estas grabaciones estarán a cargo de vigilantes de seguridad o, en su caso, guardas rurales, y no podrán tomar *imágenes y sonidos de vías y espacios públicos o de acceso público.* Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las FCS competentes, respetando

[21] STS, *Juan Ramón Berdugo Gómez de la Torre, España* de 27 de marzo de 2017
[22] STS, *Francisco José Navarro Sanchis, España* de 10 de marzo de 2020
[23] Ley 5/2014, de 14 de abril, de Seguridad Privada. BOE núm. 83 §3649 (2014)

los criterios de conservación y custodia de estas para su válida aportación como evidencia o prueba en investigaciones.

Las grabaciones obtenidas por medio de sistemas de videovigilancia pueden afectar al contenido del derecho fundamental. Para que resulten ajustadas a la Ley será necesario que las mismas se ajusten las previsiones de la Ley Orgánica de Protección de Datos.

"*El perjuicio a la imagen no existe si no se comete un delito, como en este caso ocurre y se precisa por las Fuerzas y Cuerpos y seguridad del Estado la visualización de imágenes de personas sospechosas de la participación en el delito cometido, que es lo que en este caso ocurrió." En estos casos no estamos ante un supuesto del art. 588 quinquies LECRIM de Dispositivos técnicos de captación de la imagen por las Fuerzas y Cuerpos de Seguridad del Estado, que requiere de orden judicial, sino de medidas privadas de autoprotección del propio núcleo extensivo del comercio a su radio de acción más próximo en aras a disponer de medidas de vigilancia y prevención del delito" "no puede alegarse una desproporción en el uso del contenido de las imágenes obtenidas en las cámaras de grabación instaladas con arreglo a la protección de datos y a la regulación específica en la materia, y, como se ha expuesto, por razones de prevención del delito*." (STS 20-12-2019)[24] (también STC nº 39/2016, de 3 de marzo)[25].

B) En lugares privados:

Con esto llegamos a la captación de imágenes en espacios no privados desde espacios públicos. Cuando la captación de imágenes comprometa la intimidad de las personas se exige autorización judicial para la adopción de la medida. Aplicable a captación de imágenes del interior de un domicilio desde su exterior.

"*protección constitucional de la inviolabilidad del domicilio, cuando los agentes utilizan instrumentos ópticos que convierten la lejanía en proximidad, no puede ser neutralizada con el argumento de que el propio morador no ha colocado obstáculos que impidan la visión exterior -como cerrar cortinas o plegar persianas, por ejemplo-*." "*protege, tanto frente la irrupción no consentida del intruso en el escenario doméstico, como respecto de la observación clandestina de lo que acontece en su interior si para ello es preciso valerse de un artilugio técnico de grabación o aproximación de las imágenes. El Estado no puede adentrarse sin autorización judicial en el espacio de exclusión que cada*

[24] STS, *Vicente Magro Servet, de España*, de 20 de diciembre de 2019
[25] STC, *Juan Antonio Xiol Rios*, España de 3 de marzo de 2016

ciudadano dibuja frente a terceros.", lo que conlleva a determinar el modo de aproximación de la imagen con la utilización de algún medio técnico*, "se vulnera esa prohibición cuando sin autorización judicial y para sortear los obstáculos propios de la tarea de fiscalización, se recurre a un utensilio óptico que permite ampliar las imágenes y salvar la distancia entre el observante y lo observado."* es de entender que la intromisión depende de la distancia o del medio empleado para realizar la observación directa, entendiendo que si el morador no impide la visión, como por ejemplo unas cortinas, se debe entender que al paso por pequeña distancia no se está entrometiendo, pero si por el contrario, desde la lejanía utilizo algún medio técnico, se debe entender que sí, *"cuando los agentes utilizan instrumentos ópticos que convierten la lejanía en proximidad, no puede ser neutralizada con el argumento de que el propio morador no ha colocado obstáculos que impidan la visión exterior*" "*existe violación de los derechos a la intimidad o a la inviolabilidad del domicilio cuando no se emplean instrumentos que sitúen al observante en una posición de ventaja respecto del observado. La simple toma de fotografías, sin valerse de objetivos de amplia distancia focal, no tiñe de ilicitud el acto de injerencia*"

"*Es cierto que ningún derecho fundamental vulnera el agente que percibe con sus propios ojos lo que está al alcance de cualquiera. El agente de policía puede narrar como testigo cuanto vio y observó cuando realizaba tareas de vigilancia y seguimiento… En efecto, la tutela constitucional del derecho proclamado en el apartado 2 del art. 18 de la CE protege, tanto frente la irrupción no consentida del intruso en el escenario doméstico, como respecto de la observación clandestina de lo que acontece en su interior, si para ello es preciso valerse de un artilugio técnico de grabación o aproximación de las imágenes… se vulnera esa prohibición cuando sin autorización judicial y para sortear los obstáculos propios de la tarea de fiscalización, se recurre a un utensilio óptico que permite ampliar las imágenes y salvar la distancia entre el observante y el observado". "Cuando, por el contrario, tal obstáculo no existe, como en el caso de una ventana que permite ver la vida que se desarrolla en el interior de un domicilio no es necesaria una autorización judicial para ver lo que el titular de la vivienda no quiere ocultar a los demás* ". (STS 329/2016. De 20 de abril de 2016. Prismáticos)[26].

[26] STS, *Manuel Marchena Gómez, España* de 20 de abril de 2016

"*No estarían autorizados, sin el oportuno plácet judicial, aquellos medios de captación de la imagen o del sonido que filmaran escenas en el interior del domicilio prevaliéndose de los adelantos y posibilidades técnicas de estos aparatos grabadores, aun cuando la captación tuviera lugar desde emplazamientos alejados del recinto domiciliario, ni tampoco puede autorizarse la instalación de cámaras en lugares destinados a actividades donde se requiere la intimidad como las zonas de aseo." "Pero si se trata de la grabación de imágenes en lugares públicos, aún de acceso restringido, no se requiere autorización judicial*." (STS 921/2020, de 10 de marzo de 2020[27])

Cuando se trate de captar escenas que puedan observarse sin la necesidad de dispositivos técnicos específicos y que no formen parte de la intimidad del sujeto, no necesitan autorización judicial. Es decir, cuando se vea desde fuera del domicilio sin más medios que los naturales. La toma de fotografías sin zoom ni formas de ampliar lo que los propios agentes estén viendo no necesita autorización judicial. Sin embargo, si emplean otros medios, como unos prismáticos o un zoom de una cámara, sí necesitan autorización judicial (SSTS nº 354/2003, de 13 de marzo[28] y 329/2016, de 20 de abril, SSTS nº 913/1996, de 25 de noviembre[29] y 453/1997, de 15 de abril)

1.2. Motivación de la medida:

En cualquier caso, la adopción de esta medida está sujeta a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad como medio imprescindible para alcanzar el bien social preferente de poder probar así el delito.

Es necesario que la medida:

- Resulte necesaria para facilitar la identificación de la persona investigada, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos.

- En caso de que afecte a terceros, debe ocurrir que de otro modo se reduzca de forma relevante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación. La regla general es que esta medida no puede afectar a terceros, por

[27] STS, *Julián Artemio Sánchez Melgar, España* de 10 de marzo de 2020
[28] STS, *Julián Sánchez Melgar, España* de 13 de marzo de 2003
[29] STS, *Luis Martínez – Calcerrada Gómez, España* de 11 de noviembre de 1996

lo que para poder exceptuarla se debe acreditar el criterio de excepcionalidad, justificándose estas circunstancias detalladamente en el oficio policial.

- A modo general, solo se justifica la medida por motivos de prevención y/o investigación del delito

Estos principios deben motivarse en los oficios en los que se decide la toma de estas medidas puesto que posteriormente se obligará al Juez Instructor a valorar su concurrencia en el momento de incorporar al procedimiento el resultado de estas. Asimismo, deberán argumentarse en los oficios de solicitud de autorización judicial cuando se requiera por la afectación de la medida a espacios privados.

Es importante que se respeten estos principios para asegurar la intimidad personal y la inviolabilidad domiciliaria para que el juez no anule las pruebas obtenidas con la medida.

1.3. DRONES:

Se toma como un medio más de captación de imágenes para las investigaciones policiales, teniendo los mismos requisitos que se han visto hasta ahora. No necesitan autorización judicial en caso de que solo capten imágenes en espacios públicos. En caso de utilizarse para captar imágenes del interior de una vivienda se considera que no son los medios naturales por los que el agente puede también observarla y, por tanto, sí necesitan autorización judicial.

2. Grabación de sonido:

Las FCSE pueden colocar o utilizar dispositivos electrónicos para captar las comunicaciones orales de los investigados, ya sea en lugares públicos o privados. **En ambos lugares es necesaria siempre la autorización judicial para la grabación de las comunicaciones orales del investigado**.

Cuando para hacer efectiva esta medida sea necesario **entrar en el domicilio**, se requerirá la autorización con una ponderación de los principios mucho más estricta y mayor valoración indiciaria (STS 718/2020, de 28 de diciembre[30]; STS 3-12-2020):

- Solo se admite para **encuentros concretos** de los que se tenga conocimiento de que van a poder producirse, indicándose los lugares de la vivienda que van a quedar afectados por la medida. Cada encuentro requiere una autorización judicial

[30] STS, *Manuel Marchena Gómez, España* de 28 de diciembre de 2020

independiente. *"Únicamente puede ser autorizada para la captación y grabación de uno o varios encuentros concretos que pueda tener el investigado con otras personas, haciendo depender el precepto de la concreción de la existencia de indicios que hagan previsible el encuentro. Se trata de no permitir la colocación general e indiscriminada de micrófonos y cámaras sin que exista un fundamento que justifique cada caso.". "Resolución motivadora habrá de concretar los encuentros cuya previsibilidad haya sido puesta de manifiesto en la investigación. No se ajustaría, por tanto, al modelo constitucional diseñado, la instalación de artilugios de grabación de la imagen o el sonido sin otro respaldo que la intuitiva esperanza de que esos encuentros van a tener lugar". "A falta de una mención expresa en la ley en esos lugares del domicilio que, por estar afectados de mayor privacidad, no estaría legitimada la colocación de estos dispositivos, el juez instructor deberá concretar el lugar de la vivienda donde tendría lugar la medida"*

- **Límite temporal ligado al encuentro concreto.** En caso de no conocerse con exactitud se pondrá, excepcionalmente, un plazo restrictivo. Para su prórroga se debe probar que va a haber otros encuentros. "*Es decir, es posible la instalación de dispositivos de grabación permanentes que se activen para "encuentros concretos", pero no de dispositivos de captación del sonido, y mucho menos de imagen, permanentemente activados. Lo que se está autorizando es la grabación de determinados encuentros, aunque tengan lugar en un determinado periodo sin que sea preciso estar pidiendo autorización para cada encuentro". "Reforzar la idea de que la autorización de la captación de las conversaciones o de las imágenes del investigado, solo adquiere significado cuando se pone en relación con encuentros previsible y de cuya programada realidad hayan llegado a tener conocimiento los investigadores. No se puede aspirar a recolectar encuentros con la expectativa de que, alguno de ellos, previo filtrado, podrá ofrecer una información de interés para la investigación. De ahí la reiterada mención al carácter concreto de los encuentros a la previsibilidad de estos.". "Dos de los investigados -matrimonio- residen en domicilio común, y el tercero -su hijo común- en otra vivienda cercana, por lo que no resulta de recibo que se autorice la grabación de las conversaciones que entre ellos pudieran tener en el primer domicilio, durante un mes, que no podrían calificarse como encuentros concretos,*

medida desproporcionada ". "Además se omite la exigencia del art. 588 quáter c) sobre el contenido de la resolución judicial que autorice la medida, al no hacer mención concreta al lugar o dependencias de colocación de los dispositivos, y resulta evidente que no puede equipararse autorizar las escuchas en el salón o cocina de la vivienda a una hora prudencial del día, motivada por su incipiente encuentro o visita de otros terceros sospechosos, que su colocación en otros lugares que, por estar afectados de mayor privacidad (por ejemplo: dormitorios, cuartos de baño) deslegitimarían la medida ".

- Solo es admitido en las investigaciones de delitos dolosos con pena mínima de 3 años de prisión, cometidos en el seno de grupo u organización criminal y terrorismo.

- Debe preverse racionalmente que el uso de esta medida aportará datos esenciales a la investigación.

En ningún caso el consentimiento del morador para la entrada en el domicilio puede extenderse para la colocación del aparato de escucha.

"Cuando afecte a la inviolabilidad domiciliaria, la resolución judicial habilitante deberá justificar, especialmente, la necesidad, utilidad, excepcionalidad y proporcionalidad, no ya de la medida, consustancial a todas las contenidas en el Título VIII, del Libro II LECRIM., sino también la limitación de los ámbitos de intimidad que será necesario llevar a cabo para la colocación del dispositivo. También es exigible ese plus de justificación en los supuestos en los que la captación y grabación, con independencia del lugar concreto donde se ubiquen los dispositivos, afecten a entornos o lugares especialmente buscados por la persona investigada para desarrollar su ámbito de intimidad." (STS 3-12-2020)

2.4 INJERENCIAS EN LOS EQUIPOS INFORMATICOS

Al abordar el registro de dispositivos o equipos informáticos, el legislador ha optado por distinguir entre:

- **Registro de los dispositivos de almacenamiento masivo de información**: es un registro estático en el que se produce la aprehensión física del dispositivo, pudiendo acceder al contenido del dispositivo o al contenido que es accesible desde el dispositivo.
- **Registro remoto sobre equipos informáticos**: es un registro dinámico en el que no se produce la aprehensión física.

Con el registro de estos dispositivos, de cualquiera de sus maneras, se consiguen aportar pruebas electrónicas al proceso, que consiste en toda la información producida, almacenada o transmitida por medios electrónicos que pueda tener efectos para acreditar hechos en el proceso, no solo en el penal.

1. Disposiciones comunes

Estos registros pueden afectar al derecho a la intimidad o al derecho al secreto de las comunicaciones, pero ambos se deben tomar como un conjunto, como el llamado derecho al entorno virtual, y debe ser en el momento de la motivación de la resolución cuando se pondere la afectación dependiendo, en el caso concreto, del derecho que vaya a verse afectado. El derecho al entorno virtual se configura como un derecho fundamental a la garantía de confidencialidad e integridad de los grupos de datos informáticos que va generando un usuario. De este modo, se deben tomar en consideración todos estos datos en conjunto, desde su multifuncionalidad, para su correcto tratamiento jurídico.

En ambos casos la autorización judicial es obligatoria, ya sea porque el registro se deriva de un registro domiciliario o de otra actuación, salvo que el afectado preste su consentimiento o se dé un caso de urgencia. De esta forma, la justificación y motivación será más intensa y detallada en caso de que afecte a diversos derechos fundamentales, o a uno con una especial intensidad; y será menos intensa cuando la intervención no incida de manera especialmente grave a un derecho fundamental, así se ha tomado como punto

de referencia para la creación de jurisprudencia por el alto tribunal, determinado en STS342/2013, 17 de abril de 2013[31].

1.1. Autorización judicial

Es el registro del dispositivo lo que vulnera derechos fundamentales del art. 18 CE, lo que no ocurre con la aprehensión o incautación de este, por tanto, solo será necesaria la autorización judicial para su registro, no para su incautación.

Como hemos comentado, es **obligatoria la autorización judicial** con independencia del derecho fundamental que se pueda ver afectado con la intervención, según el art. 588 sexies c) LECrim.

En la autorización es obligatorio que se valore y conste:

- **El alcance del registro**: Es importante que la investigación policial previa se oriente a determinar los indicios que puedan sustentar un determinado alcance del registro (por ejemplo, requerirá mayor motivación porque es necesaria una mayor injerencia en caso de terrorismo).

Nada impide que los términos fijados puedan ser ampliados en una nueva resolución si, como consecuencia del registro iniciado, apareciesen indicios que justifican la necesidad de acceder a otros datos (ver ampliación del registro).

---

[31] STS, *Manuel Marchena Gómez, España* 17 de abril 2013
"*El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y a la protección de datos (art. 18.4 CE). Pero su contenido también puede albergar -de hecho, normalmente albergará información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas*."
"La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital."

- La **naturaleza de los datos a los que se accederá**, pues puede permitir acceder a todos o, por ejemplo, solo a imágenes, solo al correo electrónico…, así se determina en la Circular 5/2019, de 6 de marzo de la Fiscal General del Estado, sobre registros de dispositivos y equipos informáticos, publicado en el BOE -A-2019 – 4244 del 22 de marzo de 2019 "*De todas formas, no debe olvidarse que la menor gravedad de la infracción puede compensarse, desde la perspectiva de la proporcionalidad, con una limitación de los datos a los que se permite el acceso. Así, mientras que una simple estafa de escasa cuantía no justificaría el pleno acceso a la totalidad de los datos íntimos del investigado que pudiera almacenar en su ordenador personal, no existiría inconveniente en considerar proporcionada la autorización judicial que concediera acceso a su actividad en internet, si este hubiera sido el medio de comisión del delito*."

"La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo… Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual". STS342/2013, 17 de abril de 2013

El **grado de afectación de los derechos del investigado**, como criterio fundamental para llevar a cabo una adecuada **ponderación de los intereses en conflicto que justifique el registro**. Ponderación que debe hacerse conforme a los principios que se establecen en las disposiciones comunes de medidas limitativas de derechos fundamentales:

- **Especialidad**: hace que no resulte lícito el registro preventivo o genérico de dispositivos sin que exista una investigación sobre un delito concreto, visto como todo lo contrario a una investigación prospectiva. De esta forma, el hecho que se atribuye a una determinada persona ha de estar basado en indicios objetivables en un doble sentido:
  - Siendo accesibles a terceros por aportar fuertes presunciones del hecho y la participación del sujeto en el mismo
  - Que proporcionen una base real suficiente para estimar que se ha cometido o se va a cometer el delito que se investiga

- **Excepcionalidad**: ilegalidad de cualquier registro de dispositivos que se llevara a cabo de manera sistemática. La excepcionalidad de la medida deberá ser apreciada juntamente con su idoneidad y necesidad.

- **Idoneidad**: solo ante la posibilidad indiciariamente acreditada de obtener con el registro datos relevantes para la investigación, podría justificarse el mismo se calificará como ilícito si se lleva a cabo de manera prospectiva.

- **Necesidad**: la diligencia a llevar a cabo debe ser necesaria en el sentido de que no pueda adoptarse una menos gravosa hacia los derechos fundamentales para la obtención de los resultados que se buscan. La necesidad se cumple en aquellos casos en los que la finalidad perseguida por la medida de investigación se viera gravemente dificultada sin el recurso a la misma.

- **Proporcionalidad**[32]: ese juicio deberá valorar la gravedad del delito, no solo desde la perspectiva de la pena que le corresponda, sino atendiendo también a la naturaleza del bien jurídico protegido y a la propia naturaleza de la mecánica comisiva y de las inevitables necesidades de su ulterior probanza por el obstáculo que supone el uso de dispositivos informáticos. De esta forma se pondera el interés de la persona afectada por la medida por verse preservado en el respeto de sus derechos fundamentales y el interés público y de terceros, lo cual también se manifiesta en la intensidad de los indicios existentes y la relevancia del resultado perseguido por la

[32] STS, *José Manuel Maza Martín, España* de 9 de diciembre de 2015
"Cuando se trata de infracciones cometidas mediante la utilización de equipos informáticos la diligencia tendente a su ocupación y al examen de sus contenidos debe considerarse proporcionada, no tanto en función de la pena eventualmente aplicable sino de la propia naturaleza de los hechos investigados, de su mecánica comisiva y de las inevitables necesidades para su ulterior probanza -que el registro de la vivienda donde se encuentran los instrumentos o efectos del delito resulte imprescindible para la averiguación de los hechos y la obtención de los elementos probatorios precisos para su acreditación-." "Evidentemente, cuando de infracciones cometidas mediante la utilización de equipos informáticos se trata, la diligencia tendente a su ocupación y al examen de sus contenidos, ha de considerarse como proporcionada, no tanto en función de la pena eventualmente aplicable sino de la propia naturaleza de los hechos investigados, de su mecánica comisiva y de las inevitables necesidades para su ulterior probanza. " " en esta clase de delitos, la posible volatilidad de las pruebas documentales puede aconsejar claramente en numerosos supuestos una rápida intervención tendente a su más pronta ocupación, sin las demoras que produciría una investigación más amplia, cuando, como queda dicho, las solventes sospechas acerca de la actividad ilícita llevada a cabo mediante los equipos ubicados en la vivienda objeto de registro, venían avaladas por las concretas y autorizadas referencias de las que la Policía disponía" STS5213/2015, de 9 de diciembre de 2015.

restricción del derecho. Así se ha determinado en STS 5213/2015 de 9 de diciembre de 2015.

Si esta intromisión la llevamos a un ámbito laboral se debe determinar qué No se puede considerar el control genérico que el empresario hace sobre los medios electrónicos del trabajador en su jornada laboral (correo electrónico o uso de internet) pueda regir las mismas garantías que en aquellos casos en los que la causa que motiva el acceso al espacio de privacidad del trabajador sea la sospecha fundada de la existencia de un hecho delictivo.

El empresario no puede acceder al ordenador de forma genérica para prevenir delitos, pero es diferente el caso en el que la conducta del trabajador sea la que motive el acceso. Esta conducta puede ser, por ejemplo, una evidencia de que el trabajador no está rindiendo los suficiente en su puesto y por ello se accede a los dispositivos informáticos o que, por el contrario, la conducta sea identificativa de alguna posible actividad delictiva.

De esta manera, el acceso por parte del empresario de forma oculta al contenido del correo electrónico del trabajador ante las sospechas de la posible comisión de un hecho delictivo se debe entender un control excepcional y por ello se le deben aplicar las exigencias del criterio de proporcionalidad.

2. Registro de dispositivos de almacenamiento masivo de información

2.1. Definición y alcance: Los dispositivos de almacenamiento de datos son la unión de una serie de componentes que tienen la capacidad de escribir, conservar y posteriormente recuperar o leer datos en un soporte de almacenamiento. Por ejemplo, el soporte sería un DVD, mientras que el dispositivo de almacenamiento sería la grabadora DVD. Estos se agrupan en tres grandes categorías:

- Dispositivos magnéticos (fundamentalmente, unidades de disco duro o HDD, del inglés *Hard Disk Drive*)
- Dispositivos ópticos (CD, DVD o BD)
- Dispositivos de memoria sólida o SSD (tarjetas de memoria, memorias USB, etc.)

De esta forma, la intervención puede versar sobre cualquiera de estos dispositivos, no solo ordenadores o smartphones, que pudieran tener relación con la investigación.

2.2. Autorización judicial

Concretamente, para que el registro de dispositivos de almacenamiento masivo de información sea eficaz, se deben cumplir una serie de requisitos:

- La necesidad de que la **resolución judicial** precise los términos y el **alcance del registro** tal y como se ha comentado anteriormente, bajo los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.
    - Alcance subjetivo: sujetos afectados por el registro (investigado o tercero, ya porque lo comparta o porque use uno ajeno)
    - Alcance objetivo: no solo determinando qué dispositivos pueden ser registrados y cuáles no, sino, también, la categoría o clase de datos o archivos de un dispositivo determinado a los que deberá alcanzar el registro.
- Que la resolución exprese la posibilidad de **realización de copias** de los datos informáticos. Para hacerlo, es necesario que se permita expresamente[33], prohibiendo hacerlo sin autorización judicial. Se puede llevar a cabo de dos formas:
    - **Clonado o volcado**: es una copia espejo o bit a bit de la información original y se fija con un código hash para evitar su manipulación. Puede realizarse en el momento de la incautación o en un momento posterior, que es lo más habitual. No es necesaria la presencia del LAJ, pero es altamente recomendable para garantizar la preservación de la información.
    - **Copia lógica[34]**: debe realizarse, en caso de incautación en un registro domiciliario, en ese momento, aprovechando la presencia del LAJ para dar

[33] STS, *Manuel Marchena Gómez, España* de 17 de abril de 2013
"En definitiva, la presencia del fedatario judicial en el acto del volcado de datos no actúa como presupuesto de validez de su práctica. Lo decisivo es que, ya sea mediante la intervención de aquél durante el desarrollo de la diligencia de entrada y aprehensión de los ordenadores, ya mediante cualquier otro medio de prueba, queden descartadas las dudas sobre la integridad de los datos y sobre la correlación entre la información aprehendida en el acto de intervención y la que se obtiene mediante el volcado" (STS342/2013, 17 de abril de 2013)

[34] STS, *Manuel Marchena Gómez, España* de 17 de abril de 2013
En definitiva, la presencia del fedatario judicial en el acto del volcado de datos no actúa como presupuesto de validez de su práctica. Lo decisivo es que, ya sea mediante la intervención de aquél durante el desarrollo de la diligencia de entrada y aprehensión de los ordenadores, ya mediante cualquier otro medio de prueba, queden descartadas las dudas sobre la integridad de los datos y sobre la correlación entre la información aprehendida en el acto de intervención y la que se obtiene mediante el volcado

fe de las carpetas que se copian. Además, será necesaria la presencia del interesado, ya que no se tratará de una simple diligencia de copia de archivos, sino que, en el propio acto, habrá que decidir también acerca de la selección de esos archivos, lo que requiere contradicción para garantizar el derecho de defensa del afectado.

- La necesaria **fijación por el Juez en la resolución de las condiciones para asegurar la preservación e integridad de los datos**[35], entendido como cadena de custodia. Garantizar la identidad de los dispositivos de almacenamiento masivo (que los dispositivos de los que nacen las pruebas son los mismos que fueron incautados), su integridad (que no se ha borrado ni añadido dato alguno en los mismos) y su autenticidad. Para ello es necesario su adecuado precinto y puesta a disposición judicial en el momento de su incautación:
    - Cuando se haya incautado en un registro el LAJ lo reseñará
    - En los demás casos deberá la Policía Judicial identificar adecuadamente en el acta que al efecto se levante y que deberá figurar unida al atestado que se presente, el dispositivo incautado
- La conveniencia de **evitar la incautación de los soportes de almacenamiento** cuando puedan causar al afectado graves perjuicios innecesarios que pudieran derivarse de la incautación y sea posible la obtención de una copia en condiciones que garanticen su autenticidad, salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen

2.3. Supuestos del registro:

A) Con ocasión de registros domiciliarios: Supone la incautación y acceso como consecuencia de la realización de una diligencia de entrada y registro "***la simple incautación de los dispositivos de almacenamiento masivo de información que se lleve a cabo con motivo de una entrada y registro no permite acceder a su contenido".***

Es decir, la autorización judicial de entrada y registro permite la incautación de los dispositivos (*efectos o instrumentos del delito, o libros, papeles u otros objetos que*

[35] Auto dictado por el Juzgado de Instrucción nº2 de Valladolid "*Como garantía de la autenticidad e inalterabilidad de toda la información a la que se acceda durante el registro, deberán reflejarse en el acta que se realice cuantas actuaciones de acceso y examen se verifiquen, con apoyo si se estimara conveniente en el correspondiente soporte informático mediante la realización de copias de pantalla*"

puedan servir para su descubrimiento y comprobación, dice el art. 546 LECrim), pero será **necesaria una motivación judicial especial e independiente para registrar o acceder a la información contenida en los dispositivos.**

La motivación judicial que legitime el registro de los dispositivos de almacenamiento puede realizarse en la misma resolución de entrada y registro o en otra independiente. Pero en caso de que se contemplen en la misma autorización, se deberá tener en cuenta que **la justificación del registro del dispositivo necesita un contenido propio e independiente,** por lo que se deberá fundamentar su procedencia por separado de la de la entrada y registro.

"*La jurisprudencia de esta Sala ha recordado la necesidad de que exista una resolución jurisdiccional habilitante para la invasión del derecho al entorno digital de todo investigado. Como hemos indicado supra, esa resolución ha de tener un contenido propio, explicativo de las razones por las que, además de la inviolabilidad domiciliaria, se alza la intimidad reflejada en el ordenador*." *que el Juez de instrucción exteriorice de forma fiscalizable las razones que justifican la intromisión en cada uno de los distintos espacios de exclusión que el ciudadano define frente a terceros2 (*STS nº 786/2015, de 4 de diciembre[36])

Cuando se haya autorizado y se crea necesario el registro del dispositivo en el mismo momento del registro, se hará en presencia del LAJ y del imputado en todo momento.

B) Fuera del domicilio

La incautación del dispositivo puede darse fuera del domicilio, es decir, independientemente de un registro domiciliario, por ejemplo, ante una detención. En estos casos la Policía Judicial debe poner en conocimiento del Juez la incautación de los efectos y para su acceso y registro igualmente es requisito la autorización judicial en los términos ya explicados.

En caso de que no se considere necesario analizar el contenido del dispositivo, se deberá devolver a su propietario.

[36] STS, *Manuel Marchena Gómez, España* de 4 de diciembre de 2015

C) Excepciones a la autorización judicial

A pesar de que, como hemos aclarado, es necesaria la autorización judicial, el registro de dispositivos de almacenamiento masivo de información puede darse por otras dos vías: el consentimiento del afectado o el caso de urgencia.

a) Consentimiento del afectado

El consentimiento del afectado hace que no sea necesaria la autorización judicial para el registro de dispositivos de almacenamiento de uso masivo de información. El requisito para que se dé esta situación es que el afectado tenga capacidad para prestar consentimiento y se haya hecho libre y voluntariamente.

El consentimiento puede ser expreso o tácito, al igual que en las entradas y registros. El consentimiento tácito se puede entender como el que resulta de actos que manifiesten inequívocamente la voluntad, sin que se pueda entender como consentimiento tácito la no oposición al registro.

STS nº 786/2015, de 4 de diciembre: En la que se admitió que esa voluntad tácita se dedujera del acto de facilitar la interesada la identidad de las cuentas de correo electrónico y sus claves: "*La defensa subraya que Susana sólo proporcionó a los agentes en el momento de la detención "... las cuentas y las claves, no la autorización expresa para el acceso al contenido del ordenador y, concretamente, al correo electrónico". Sin embargo, como hemos apuntado supra, el consentimiento para legitimar el acceso al contenido documentado de comunicaciones a las que ya se ha puesto término y que, en consecuencia, desbordan la protección constitucional que dispensa el art. 18.3 de la CE, puede ser otorgado mediante actos concluyentes. Y bien elocuente de la voluntad de Susana son los actos de identificación de las cuentas y entrega de las claves*."

El consentimiento podrá revocarlo el afectado en cualquier momento y no alcanzará a la extralimitación de los términos y alcance para el que fue otorgado. *Ahora bien, se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto «aún autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida»*

"Lo primero que cabe afirmar es que la autorización que el recurrente prestó para el acceso a su ordenador al propietario del establecimiento de informática, en la forma

expuesta, no puede extenderse al posterior acceso a los archivos por parte de la Policía. Tal como hemos afirmado anteriormente, el derecho a la intimidad personal se vulnera también cuando, aun autorizada su intromisión en un primer momento, se subvierten después los términos y el alcance para el que se otorgó. Como hemos visto, en el presente caso el alcance de la autorización dada se circunscribía a la manipulación por parte de dicho profesional del portátil para que procediera a la reparación del equipo informático, lo que no puede erigirse en legitimación para una intervención posterior realizada por personas distintas y motivada por otros fines.

→ En caso de que el afectado esté DETENIDO: En los casos en los que el afectado se encuentre detenido, aplicando la doctrina jurisprudencial elaborada para los casos de registro domiciliario, no será precisa la asistencia del letrado para llevar a cabo el registro del dispositivo, lo que sí es recomendable es la presencia del LAJ.

Sí es necesaria la asistencia de letrado para obtener el consentimiento del afectado para acceder al dispositivo si no existiera autorización judicial. Pero, concretamente, en caso de que el detenido proporcione las claves del dispositivo, tampoco es necesaria la asistencia de letrado ya que en este caso se ve como un simple acto de facilitación del acceso, no como el consentimiento.

STS 2160/2020[37] de 15 de junio: "*Sin embargo estimamos que no tiene la misma trascendencia comunicar voluntariamente las claves de acceso a un equipo informático. Por hacer un símil que permita visualizar la diferencia, no es lo mismo entregar las llaves para que se pueda acceder a un domicilio, que entrar y registrar ese domicilio. La entrega de llaves es un acto previo que facilita la entrada y que evita que se tenga que acudir a otros medios (forzamiento de cerradura, por ejemplo), pero la afectación del derecho a la inviolabilidad del domicilio se produce cuando se entra en él y se registra. Lo mismo ocurre con la entrega de las claves. La entrega voluntaria de las claves facilita el acceso a la información ya que, en otro caso, habrá de acudirse a otros procedimientos para conseguir el acceso, pero esa entrega voluntaria no autoriza a que la policía acceda a la información alojada en el ordenador. Para esto último se precisa autorización judicial." "Por último, no es requisito que, en caso de detención, la cesión voluntaria de las claves se haga a presencia de Letrado y no lo es porque la ley no lo exige y porque la*

[37] STS, *Eduardo de Porrees Ortiz de Urbina, España* de 15 de junio de 2020

manifestación del detenido tiene un alcance muy limitado y no supone per se una injerencia en el derecho a la intimidad, ya que para acceder al contenido de la información alojada en el ordenador no basta con el consentimiento del interesado sino que se precisa autorización judicial. Sin embargo, la asistencia de Letrado es muy recomendable y es expresión de una buena práctica porque aleja toda sombra de sospecha sobre las condiciones en que se produjo esa comunicación. Ya hemos dicho que la colaboración del detenido debe ser, en todo caso, libre, voluntaria y ajena a presiones ambientales, por lo que la presencia de Letrado y la ausencia de protesta en la práctica de la diligencia será un indicador de suma relevancia para evitar toda controversia posterior"

→ **Dispositivos usados simultáneamente por varias personas**: Tienen una particularidad y es que resultará válido el consentimiento otorgado por cualesquiera de ellas, incluso, para el examen de los datos íntimos de las otras, salvo cuando exista conflicto de intereses entre ellas.

"Q*uien incorpora fotografías o documentos digitales a un dispositivo de almacenamiento masivo compartido por varios es consciente de que la frontera que define los límites entre lo íntimo y lo susceptible de conocimiento por terceros, se difumina de forma inevitable*" "*Con independencia de ello, se trata de una prueba proporcionada por un particular a los agentes de la autoridad sin que esa entrega haya sido concebida como un mecanismo de elusión de las garantías que el sistema constitucional reconoce para la protección de los derechos a la intimidad y al entorno virtual*." (STS nº 287/2017, de 19 de abril)[38]

b) Caso de urgencia

Existe la posibilidad, en virtud del art. 588 sexies c) LECrim, de que la Policía Judicial pueda registrar dispositivos de almacenamiento masivo de información sin previa habilitación judicial en los casos de urgencia en los que, además, se aprecie un interés constitucional legítimo que haga imprescindible la medida y, siempre, con convalidación posterior del Juez. Este art. se aplica son independencia del derecho fundamental al que afecte el registro.

Por lo tanto, se obliga a la Policía Judicial a poner el registro inmediatamente en conocimiento del juez y, como máximo, en el plazo de 24 horas.

[38] STS, *Manuel Marchena Gómez, España* de 19 de abril de 2017

La LECrim condiciona la validez del registro policial previo a la concurrencia de cuatro requisitos:

- **Urgencia**, como la que resulta necesaria para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias.

- **Interés constitucional legítimo** que haga imprescindible la medida. Es necesario que la medida persiga a alguna de las siguientes finalidades establecidas por la jurisprudencia (TC y TS): la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás.

- **Comunicación posterior al Juez** en la forma y plazos que se establecen →

    - Requisito formal: mediante un escrito en el que se dé cuenta de las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado.

    - Requisito temporal: de inmediato y como máximo 24h. Se ha de levantar acta de registro en el que se haga constar el momento en el que se dio el mismo.

- **Convalidación judicial posterior de la medida.**

De adoptarse sin consentimiento del afectado y sin autorización judicial, han de acreditarse razones de urgencia y necesidad que hagan imprescindible la intervención inmediata y respetarse estrictamente los principios de proporcionalidad y razonabilidad"... (STS 10-3-2016)

<u>c) Datos que afectan derecho a la intimidad vs secreto comunicaciones</u>

Con anterioridad a la reforma de la LECrim se entendían los derechos a la intimidad y secreto de las comunicaciones por separado y se actuaba de acorde al derecho que se fuera a ver afectado en el caso concreto, permitiendo que se afecte al derecho a la intimidad sin necesidad de autorización judicial cuando concurrieran razones de urgencia, necesidad y proporcionalidad. Pero esta doctrina ya no es válida. La nueva doctrina responde a la necesidad de otorgar un **tratamiento unitario para conjunto de derechos** que convergen cuando se hace uso de uso de un ordenador, *smartphone,* o de modernos

sistemas de comunicación telemática y superar así los problemas que pudiera causar un tratamiento diferenciado. De esta forma, se deberá aplicar el régimen de **necesidad de autorización judicial** previa que se regula en la LECrim para el registro de todos los dispositivos de almacenamiento masivo de información con independencia de que solamente alcance el derecho a la intimidad.

*"La necesidad de esta autorización judicial (subsidiaria del consentimiento: si el afectado accede de forma libre, no hay cuestión) obedece a la consideración de estos instrumentos como esferas de almacenamiento de una serie compleja y densa de datos que afectan de modo muy variado a la intimidad del investigado. La contemplación disgregada de cada una de esas realidades con regímenes de protección diferenciados resultaría ineficaz. Permitido, por ejemplo, el acceso directo de los agentes policiales a estos instrumentos para investigar datos únicamente protegidos por el derecho a la intimidad (v.gr., los contactos incluidos en la agenda), no se podría acceder o consultar también otros datos tutelados por el derecho a la inviolabilidad de las comunicaciones albergados en el mismo dispositivo. El Legislador con buen criterio ha optado por otorgar un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando ese derecho constitucional de nueva generación, el derecho a la protección del propio entorno virtual. (*STS n.º 489/2018 de 23 de octubre)[39]

2.4. Ampliación del registro (repositorios telemáticos de datos)

Los repositorios telemáticos de datos son dispositivos de almacenamiento masivo de información a los que se tiene acceso de manera telemática (cloud computing: sustituir los dispositivos de almacenamiento masivo de información clásicos por el almacenamiento en servidores de internet.). En todos estos casos, aunque no se trata de servicios específicamente destinados al almacenamiento de datos personales, se generan depósitos de información en alojamientos externos a los que se accede a través del dispositivo o sistema propio del usuario.

El legislador prevé la posibilidad de su registro ante la probabilidad de que puedan albergar datos relevantes para la investigación de los delitos.

[39] STS, *Antonio del Moral García, España* de 23 de octubre de 2018

Esta **posibilidad de registro debe aparecer suficientemente fundada y motivada en autorización judicia**l, bien desde un primer momento, lo que provocará que el Juez autorice su registro ya en la resolución inicial que dicte (art. 588 sexies a.1), bien como consecuencia de los datos que se obtengan con el registro ya autorizado, lo que dará lugar a la ampliación del registro que regula el art. 588 sexies c.3.

Este art. permite el acceso a otro sistema informático, sin especificar la titularidad propia o ajena del mismo, eso sí, condicionándolo siempre a *que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este.*

Este art. también prevé la posibilidad de que la policía judicial pueda llevar a cabo igualmente el registro ante un caso de urgencia, debiendo avisar inmediatamente al juez o, como máximo, en un plazo de 24 horas. Se dará ante situaciones de peligro inminente de que la información pueda desaparecer.

El procedimiento para llevar a cabo en estos casos, por tanto, depende de si se cuenta con las claves para acceder a este sistema o no. En caso de que se tengan de forma lícita, ya sea porque el dispositivo no cuenta con contraseñas o porque estén en poder de la autoridad, se podrá acceder directamente si se cuenta con autorización judicial, garantizando, al igual que en la regla general, la integridad de la información adquirida. En cambio, en caso de que no se cuente con las contraseñas, no se podrá realizar el registro de la información directamente, sino que será necesario acudir a la empresa que gestione el servicio para que permita el acceso a la información, las cuales tienen que actuar bajo el deber de colaboración.

"En este sentido, tampoco el hecho de que el recurrente permitiera, a través del programa «eMule» este acceso de otros usuarios a sus archivos, puede erigirse en una suerte de autorización genérica frente a posteriores y distintas injerencias en el ámbito reservado de su intimidad, a pesar de que ha sido éste el argumento utilizado aquí tanto por la Audiencia Provincial de Sevilla como por la Sala Segunda del Tribunal Supremo. En efecto, además de que el acceso a los expresados archivos sólo es factible para los usuarios que tengan instalada su misma aplicación, es lo cierto que la Policía tan solo tiene conocimiento de la utilización del referido programa cuando accede al ordenador, siendo así que, conforme hemos expuesto, las circunstancias que permiten afirmar la existencia del presupuesto habilitante para penetrar en la esfera de la intimidad del titular del derecho deben evaluarse y apreciarse ex ante, sin que dicho acceso pueda

justificarse ex post a partir de hechos sólo descubiertos después y como consecuencia del mismo". (STS 173/2011 de 7 de noviembre de 2011)[40]

→ Datos en la nube almacenados en el extranjero: El problema viene cuando estos datos se encuentran almacenados en otro país. En caso de que se cuente con el permiso del usuario para acceder o con las claves se actúa según el procedimiento explicado, pero si es necesaria la colaboración de quienes prestan el servicio para acceder a los datos la situación es diferente puesto que la solicitud de cooperación de dichos prestadores podría tener que realizarse a través de los instrumentos de cooperación judicial penal internacional.

Cuando los datos se encuentren en un país miembro de la Unión Europea, se suelen solicitar los datos a dicho país a través de la Orden Europea de Investigación; mientras que, cuando los datos se encuentren en un país no miembro, se usa la Cooperación Judicial Recíproca (MLA). El problema es que estas técnicas, aunque funcionan bien para otras formas de investigación, en caso de obtener pruebas electrónicas pueden suponer demasiada lentitud, por lo que normalmente se obtienen a través de la cooperación voluntaria entre las autoridades judiciales y los prestadores de servicios de internet (sobre todo en EEUU, cuya legislación lo permite). En la actualidad, la UE está regulando una nueva forma de solicitar y obtener esta información de manera más rápida y directa, a través de lo que se llamará Orden Europea de Retención (European Preservation Order).

2.5. Deber de colaboración

El deber de colaboración con las autoridades y agentes encargados de una investigación afecta al registro en cualquier tipo de dato del entorno virtual. Este deber se impone no solo a las operadoras de telecomunicaciones sino también a cualquier tercero que pudiese facilitar el acceso a este tipo de dispositivos como pueden ser los prestadores de servicios, el fabricante, o cualquier persona física o jurídica que tuviere conocimiento del sistema.

El alcance de este deber supone la obligación de facilitar información, pero nada más (ej: no se puede pedir crear software para entrar en el dispositivo).

Están excluidas de este deber las personas a las que les pudiera acarrear una carga desproporcionada, el investigado o encausado, las personas que están dispensadas de la

[40] STC, *Elisa Pérez Vera, España* de 14 de noviembre de 2011

obligación de declarar por razón de parentesco y a aquellas que no pueden declarar en virtud del secreto profesional.

- La carga desproporcionada hace referencia a la dificultad técnica del concreto mandato y a la existencia de firmes compromisos por parte de la compañía con la clientela que se viera sacrificados si colaboraran y dicho incumplimiento supondría una desventaja competitiva frente a su competencia.

- Además, tampoco son sujetos obligados por este deber de colaboración ni el fabricante del dispositivo ni el diseñador o proveedor del software, cuando sean distintos al prestador de servicios.

3. Registros remotos sobre equipos informáticos

Los registros remotos de dispositivos informáticos son una forma de acceder a la información de un dispositivo, vigilar la actividad y obtener pruebas a través de programas informáticos que se instalan en el dispositivo que se quiere conocer. De esta forma, se prolonga en el tiempo la injerencia, afectando más gravemente a los derechos del investigado. Este se regula en el art. 588 septies LECrim.

Así, existen dos notas esenciales que concurren en los registros remotos y no en los registros directos: la clandestinidad y el carácter dinámico del registro, puesto que los registros remotos pueden conocer, no solo lo que existe en un dispositivo en un momento determinado, sino también lo que se va añadiendo o borrando del mismo durante el tiempo que dure la medida

Por esta mayor afectación a los derechos fundamentales, esta medida es más estricta, lo que se manifiesta en que en este caso no sea posible el registro policial convalidado posteriormente por el Juez, ni en los casos de urgencia, ni cuando se trate de ampliar el registro a otros sistemas, como ocurría con los registros directos.

3.1. Sistemas de acceso

El art. 588 septies a regula la posibilidad de realizar registros remotos de equipos informáticos a través de dos concretas técnicas:

- La utilización de datos de identificación y códigos: utilizar las propias contraseñas del investigado para acceder.

- La instalación de un *software*: son programas que permiten a la autoridad escanear un disco duro y otras unidades de almacenamiento y remitir de forma remota y automatizada el contenido a la autoridad responsable de la investigación. Lo normal es que se realice con un "troyano", es decir, un virus espía que es un programa enmascarado bajo otra denominación, que una vez abierto despliega su contenido en el ordenador del investigado sin su conocimiento. Es posible que se necesite autorización judicial de entrada en el domicilio del investigado para manipular directamente su equipo informático e instalarlo.

3.2. Ámbito de aplicación

Otra exigencia de esta diligencia es que solo es posible su aplicación para la investigación de alguno de los **siguientes delitos,** lo que ayudará a motivar el juicio de proporcionalidad:

- Delitos cometidos en el seno de organizaciones criminales
- Delitos de terrorismo
- Delitos cometidos contra menores o personas con capacidad modificada judicialmente
- Delitos contra la Constitución, de traición y relativos a la defensa nacional
- Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación

3.3. Resolución judicial

El art. 588 septies a.2 exige **necesariamente autorización judicial,** con un determinado contenido, debiendo precisar:

- **El objeto del registro**: que se especifiquen los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de estos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.
- **El alcance del registro**: será posible que el registro recaiga sobre un dispositivo o repositorio de datos concreto, o sobre todo el sistema informático del investigado.

- **La forma de acceso al sistema** con especificación del *software* utilizado.
- **Los agentes autorizados** para la ejecución de la medida.
- la autorización, en su caso, para **realizar copias y conservarlas**, que puede limitarse a permitir el simple visionado y conocimiento de los datos o, por el contrario, puede consentir la grabación de estos.
- Las **medidas de aseguramiento** de los datos registrados.

En los casos del registro remoto no será posible, como sí lo era en los registros directos, llevar a cabo la ampliación del registro sin autorización judicial previa en caso de urgencia, ya que el caso de urgencia no se contempla en esta diligencia. De esta forma, si se acuerda la ampliación del registro deberá antes el Juez dictar una nueva resolución habilitante del mismo, que estará sujeta a idénticos requisitos que la resolución original que autorizó el registro del sistema principal.

3.4. Duración de la medida

La duración que establece la LECrim para esta diligencia es de un mes como máximo, prorrogable por partes iguales hasta un periodo máximo de 3 meses.

La fijación concreta del tiempo de duración de la medida vendrá determinada por la valoración conjunta de los principios rectores en el caso concreto. De esta manera, habrá que atender a la necesidad de la medida, la imposibilidad de progresar en la investigación por otros medios y la gravedad de los hechos objeto de investigación, en relación con el preciso alcance que, para el caso concreto, se fije a la medida.

En consecuencia, los plazos que establece el art. 588 septies c se computarán, tanto en su duración inicial como en la duración total, desde la fecha de la resolución judicial autorizante y no desde el comienzo efectivo del registro.

3.CONCLUSIONES

Podríamos pensar que los derechos fundamentales están protegidos jurídicamente por nuestra Constitución Española y que todo aquel que ataque a los mismo debe tener las consecuencias legales consensuadas por nuestros legisladores, incluso con el derecho de retracto.

La duda que subyace socialmente es aquella que se exige como persona propietaria de la intimidad, del honor y de la imagen, derechos que se defienden constitucionalmente que entrar directamente en choque con los metadatos que voluntariamente compartimos de nuestra intimidad, de nuestros hábitos, de nuestras necesidades, inquietudes y de nuestra forma de pensar, exponemos nuestra vida milimétricamente ante una sociedad, bien sea digital o virtual en la que no reparamos y que puede llegar a hacer más daño que la difamación o injerencia que se haga de un derecho como es la intimidad o el honor.

Cabe pensar, y para eso se ha legislado en el ámbito de la tecnología, en el derecho al olvido, derecho que no siempre se consigue ya que podemos llegar a lograr la eliminación de unos parámetros de la red, pero obviamos inocentemente la difusión de nosotros mismos cuando damos permiso a todas las apps´s que hoy en día tenemos en nuestros teléfonos móviles.

En este trabajo se ha hablado de los principios necesarios para influir en la geolocalización con fines de investigación, pero debemos entender que hoy en día cualquier persona voluntariamente comparte su geolocalización de una manera total, sin llegar a determinar que o quien maneja esos datos que estamos compartiendo. Cualquier dispositivo que llevemos con nosotros, incluso que podamos llegar a utilizar determina una geolocalización que compartimos sin saber los fines de ello.

Vivimos en una sociedad de auge en la Inteligencia Artificial que no está regulada y que escapa a la legislación tanto nacional como internacional. Escapa a la determinación de la fina línea de legalidad e ilegalidad.

Deberíamos determinar dónde están los principios fundamentales que determinan compartir tu mapa sentimental y funcional, no solo cuando compartes una foto en las redes sociales, sino de los datos ocultos que damos a diario y que hoy en día todavía no hemos determinado jurídicamente su funcionalidad.

En este sentido confrontan las vertientes judiciales con las sociales en el momento con la realización de una limitación de derechos realizada por parte de las FCSE que se deben ajustar, como no puede ser de otra manera a la legislación vigente mantenida tras las diferentes sentencias emitidas por el TS. Por ello no cabe duda de que la restricción de ciertos derechos fundamentales en un ámbito judicial, pasan por unos principios rectores de riguroso cumplimiento como son los principios de **especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad**. Fuera de estos requisitos las FCS tiene la prohibición absoluta de realizar injerencias a las limitaciones de los derechos fundamentales, y es por eso por lo que en muchas ocasiones, el ímpetu de la realización del beneficio hacia la seguridad nacional o pública, se han visto demasiadas diligencias revocadas por el TS, por el simple hecho de una posible debilidad a la hora de mantener alguno de los completos principios.

Esta nueva regulación del art. 588 de la LECrim, ha puesto de manifiesto la necesidad de legislar de acorde al avance de las nuevas tecnologías sin dejar atrás el absoluto respeto hacía los derechos fundamentales de la persona.

No obstante, en muchas ocasiones cuesta entender sentencias que rechazan las medidas tomadas como limitadoras de algún derecho fundamental, con posibles repercusiones hacía los miembros de las FCS, a la misma vez que vemos como inocentemente se comparten y se exponen datos, geolocalizaciones, imágenes o videos sin ser meramente conscientes de ello.

A lo largo de mis 29 años de experiencia profesional en FCSE, donde 22 de ellos los he dedicado a la investigación y a la instrucción de diligencias, he podido comprobar como en muchas ocasiones, por más seguridad que se tengan de los hechos, el recorrido del delito no llega a su plenitud y cuesta demostrar ciertas acciones que, aunque vengan determinadas en la diferente legislación de nuestro país, a través del aprendizaje de la jurisprudencia se ha visto diluido el argumento expuesto.

Nuestro ordenamiento jurídico radica en el principio de jerarquía normativa y en muchas ocasiones, se han encontrado confrontaciones legislativas que chocan con el espacio social donde nos movemos, por ello en ocasiones hemos visto como se ha legislado a golpe social, en ocasiones con un cierto beneficio hacia el perjudicado o la víctima y en otras ocasiones al amparo de los Derechos Humanos y derechos de detenidos.

Cabe pensar, y sería un debate abierto, donde a priori todas las partes darían sus argumentos razonados y convincentes, que ciertas medidas favorecedoras del derecho de la persona detenida impiden el desarrollo de las investigaciones en el ámbito policial. Cualquiera se pararía a plantearse donde está el derecho de la victima en contra partida con el derecho del detenido.

La modificación realizada sobre el art. 588 de la LECrim a través *de 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*, ha tratado de enmendar situaciones, hasta el momento poco abordadas legislativamente pero si puestas en entredicho a través del TS. No en vano, actualmente tenemos determinados los principios rectores del recorrido del delito para la imposición de una medida, siempre dirigida por los magistrados y apoyada por el garante legislativo de la figura del fiscal, y que guían de forma clara a la hora de la realización de las investigaciones policiales con el fin de poder tener las cosas claras ante los Juzgados de Instrucción, guiando el camino para que no sean tumbadas, ciertas medidas, en el TS, teniendo claro que la forma de iniciar las investigaciones parte de unos requisitos legislativos compatibles con la jurisprudencia.

Al término del presente trabajo, como inicio de algo más laborioso de cara a facilitar la doctrina policial, se abren lagunas enfocadas a la inteligencia artificial y la regulación de esta, donde el ámbito social gira por un camino, a través del consentimiento que en ocasiones se hace de difícil entendimiento en la legislación normativa, por lo que nos podemos llegar a encontrar ante la perpetración de supuestos delitos realizados por maquinas dirigidas informativamente, donde la manipulación humana no llegue a determinar actuaciones concretas, entendiendo que el TS debe tomar medida proactiva para poder solventar posibles lagunas jurídicas donde nos lleve esta nueva era de avances informáticos.

4.FUENTES NORMATIVAS

Constitución Española, BOE núm. 311 § 31229 (1978)

Ley 25/2007, de 18 de octubre de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación.

DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo

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 medias de investigación tecnológicas, BOE núm. 239 §10725 (2015)

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, BOE núm. 260 §6036 (1882)

Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. BOE, núm. 186 §17574 (1997)

Ley 5/2014, de 4 de abril, de Seguridad Privada. BOE núm. 83 §3649 (2014).

Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registros de dispositivos y quipos informáticos. BOE, núm. 70 §4244 (2019).

5.BIBLIOGRAFÍA

5.1 Jurisprudencia

STC 0045-2004-AI

STS 141/2020, de 13 de mayo

STS 610/2016, de 7 de julio

STS 7-7-2016

STS 7-7-2016, TEDH

STS 610/2016 de 7 de julio de 2016

STS 731/2013, de 7 de octubre

STC 94/1999, 31 de mayo

STS 28-1-2014

STS 5-6-2013

STS 272/2017, de 18 de abril

STS 200/2017, de 27 de marzo

STS 10-3-2020

STS 20-12-2019

STC 39/2016, de 3 de marzo

STS 20-4-2016.

STS 10-3-2020

SSTS 354/2003, de 13 de marzo

SSTS 913/1996, de 25 de noviembre

STS 718/2020, de 28 de diciembre

STS 3-12-2020

STS 562/2007, 22 junio

STS 141/2020, 13 de mayo

STS 342/2013, 17 de abril de 2013

STS 5213/2015 de 9 de diciembre de 2015

STS 786/2015, DE 4 de diciembre de 2015

STS 2160/2020 de 15 de junio de 2020

STS 287/2017, de 19 de abril de 2017

STS 489/2018 de 23 de octubre de 2018

STS 173/2011, de 7 de noviembre de 2011

5.2. Doctrinal

- Parlamento Europeo "El Derecho al respeto de la vida privada: Los retos digitales, una perspectiva del Derecho Comparado." https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628261/EPRS_STU(2018)628261_ES.pdf (Consultado el 01/03/2021)

- Doctrina jurisprudencial año 2016. Sala de los Penal Tribunal Supremo. Gabinete Técnico file:///C:/Users/NAP/Downloads/20170316%20Doctrina%20jurisprudencial%20de%20la%20Sala%20de%20lo%20Penal%202016%20-%20Semestre1.pdf (Consultado 15/03/2021)

- Boletín de Jurisprudencia de Protección internacional: Segundo semestre de 2016. https://www.cear.es/wp-content/uploads/2017/05/BOLETIN-JURIDICO-CEAR-SEGUNDO-SEMESTRE-2016.pdf (Consultado el 15/03/2021)

- Derechos fundamentales afectados por la geolocalización. https://elderecho.com/derechos-fundamentales-afectados-por-la-geolocalizacion (Consultado el 16/03/2021)

- La reproducción de imágenes y sonidos como medios de prueba. https://www.economistjurist.es/articulos-juridicos-destacados/la-reproduccion-de-imagenes-y-sonidos-como-medios-de-prueba/ (Consultado el 20/03/2021)

- La infiltración policial: en el límite del Estado de Derecho. El inminente agente encubierto informático. https://noticias.juridicas.com/conocimiento/articulos-

doctrinales/10222-la-infiltracion-policial:-en-el-limite-del-estado-de-derecho-el-inminente-agente-encubierto-informatico/ (Consultado el 20/03/2021)

6.OTROS RECURSOS EMPLEADOS

En la elaboración del presente trabajo, además de los artículos doctrinales y la diferente jurisprudencia analizada, se han empleado los otros recursos de difícil señalamiento en este apartado, dado que se refieren a la experiencia laboral de 29 años de servicio en la FCSE, del que suscribe, y es por ello por lo que los artículos doctrinales han sido utilizados en menor medida que el extenso análisis realizado de la jurisprudencia.

7.ANEXOS