TECNOLOGÍA DE GEOLOCALIZACIÓN Y SEGUIMIENTO AL SERVICIO DE LA INVESTIGACIÓN POLICIAL. INCIDENCIAS SOBRE EL DERECHO A LA INTIMIDAD

Francisco de la Torre Olid
Catedrático de Derecho Civil
Universidad Católica San Antonio de Murcia

Francisco García Ruiz
Unidad Técnica de Policía Judicial de la Guardia Civil
Oficial de Enlace OCN-Interpol España

RESUMEN

El presente trabajo analiza el potencial de los nuevos medios técnicos de localización y seguimiento al servicio de las investigaciones policiales analizando las tensiones que se producen sobre el derecho a la intimidad debido a la deficiente regulación de la materia.

Palabras clave: Intimidad, tecnovigilancia, geolocalización, seguimiento, injerencia, protección de datos, patrón de comportamiento.

ABSTRACT

This work is aimed to measure the impact of the new technical means for tracking and location of people applied to the police research by ananlizing the tensions over the right of privacy due to the deficient regulation in Law.

Key words: *Privacy, high-tech surveillance, geolocation, tracking, interference, data protection, pattem of behavior.*

SUMARIO: I. INTRODUCCIÓN. II. EL DERECHO A LA INTIMIDAD. III. MEDIDOS Y TÉCNICAS DE LOCALIZACIÓN Y SEGUIMIENTO. 1. Balizas (dispositivos de control remoto). 2 Interceptación telefónica mediante software o hardware. 3. Intervención de comunicaciones vía satélite. 4. Vigilancia a través de sistema de telefonía móvil (GSM-UTMS) sistema de intervención telefónica SITEL. 5. WiFi (localización a través de puntos de acceso). 6. Localización mediante control indirecto de datos personales. 7. Sistemas de tratamiento y gestión de datos. IV. SMARTPHONE Y LOS SERVICIOS CON VALOR AÑADIDO. V. INCIDENCIA DE LOS MEDIOS TÉCNICOS DE LOCALIZACIÓN SOBRE EL DERECHO FUNDAMENTAL A LA INTIMIDAD. VI. REQUISITOS DE LEGITIMACIÓN DE LOS MEDIOS DE LOCALIZACIÓN Y SEGUIMIENTO. 1. Existencia de fin legítimo. 2. Previsión Legal suficiente. 3. Autorización judicial previa. 4. Proporcionalidad de la medida. 5 Excepcionales injerencias sin necesidad de autorización judicial previa. VII. INEXISTENCIA DE REGULACIÓN LEGAL. ¿CONSECUENCIAS? VIII. CONCLUSIONES. IX. BIBLIOGRAFÍA

I. INTRODUCCIÓN

Hace tan sólo unos años la posibilidad de que un artilugio "supiese" en qué punto concreto del planeta nos encontramos, con un error de pocos metros, nos parecía ciencia ficción. Sin embargo a nadie sorprenden hoy los navegadores que portan los vehículos, esos que nos indican por qué calle circulamos, cuál es la próxima curva, dónde debemos girar, a qué velocidad nos movemos... y que, en definitiva, que saben dónde nos encontramos. Hablamos del conocido GPS.

GPS[1], la tecnología más popular, no es la única que permite la geolocalización de objetos, sino que podemos destacar otras como los sistemas de telefonía, o las comunicaciones a través de radio como la popular red WiFi, que permiten la localización de los objetos a través de los que se materializa una determinada "*comunicación*", máxime cuando se combinan varias tecnologías en un único instrumento, como ocurre con los actuales teléfonos inteligentes *smart-phones*.

Tampoco podemos obviar nuestra interacción con aquellos sistemas que requieren la previa identificación, como es el caso de cajeros automáticos en entidades bancarias, etc., que informarán, en un momento concreto, de nuestra ubicación física.

Los instrumentos y herramientas tecnológicas que permiten ubicar y seguir a una persona son hoy imprescindibles en multitud de investigaciones, especialmente aquellas relacionadas con la delincuencia organizada. Frente a la carga subjetiva de la observación y vigilancia directa del investigador sobre el objetivo, los medios técnicos proporcionan mayor objetividad y precisión así como permiten el mantenimiento de medidas de control en el tiempo con una menor dedicación de recursos humanos.

[1] GPS: (Global Positioning System: sistema de posicionamiento global) o NAVSTAR-GPS es un sistema global de navegación por satélite que permite determinar en todo el mundo la posición de un objeto concreto.

También, los medios técnicos, permiten la obtención y tratamiento de un mayor número de datos e informaciones, facilitando que los investigadores aporten mejor material probatorio con el que conformar la convicción judicial.

Ahora bien, la combinación de los sistemas técnicos que permiten localizar un objeto, y en consecuencia a la persona que lo porta o usa, pueden facilitar la ubicación casi exacta, con un error cada vez más despreciable, conocer los itinerarios seguidos, establecimientos visitados, etc., en definitiva no sólo permiten conocer su ubicación en un momento concreto sino que permiten trazar un perfil de comportamiento personal que, pudiendo ser de incuestionable utilidad para los investigadores policiales, puede ser de tal intensidad que afecte de forma severa al derecho a la intimidad y a la protección de datos de carácter personal, especialmente en su vertiente de autodeterminación informativa.

MADRID CONESA[2], en su teoría sobre el mosaico, alertó sobre el riesgo de la recopilación de datos aparentemente inocuos, pero que puestos en conexión con otros, en principio irrelevantes, pueden ser utilizados para configurar un perfil de comportamiento de una persona y hacerla transparente ante cualquier poder político. Como en un mosaico las piezas por separado no significan nada, pero encajadas unas con otras ofrecen una realidad identificable.

La sociedad actual, tras los atentados en Nueva York, Madrid y Londres ha tomado conciencia de la necesidad de intensificar la vigilancia sobre las personas, especialmente en el ámbito de la lucha antiterrorista, pero esta concienciación no debe provocar la dejación de las funciones de protección de los derechos fundamentales que corresponden al Estado, pues es incuestionable la incidencia, cada vez mayor, que la utilización de los medios técnicos de vigilancia y localización tienen sobre la privacidad, sobre el derecho fundamental a la intimidad y a la protección de datos cuando entran en concurso no sólo las tecnologías de vigilancia sino el tratamiento automatizado de la información.

No debemos olvidar que entre los medios técnicos que facilitan la vigilancia, que ahora denominamos *tecnovigilancia*, se encuentran, además de aquellos que específicamente persiguen obtener la ubicación geográfica del objetivo, otros que además que permiten la captación, almacenamiento y tratamiento de imágenes y audio. No en vano, la captación de imágenes, por ejemplo por el sistema de videovigilancia de un aeropuerto, banco, etc., sometida a un proceso de tratamiento y reconocimiento biométrico, puede dar lugar a la identificación de la persona mediante su fotografía, lo que supone el conocimiento de la identidad y su ubicación en un espacio físico y temporal concreto[3]. Sin embargo, sin olvidar aquellos sistemas que

[2] MADRID CONESA, F: *Derecho a la intimidad, informática y Estado de Derecho*, Valencia, Universidad de Valencia, 1984, pág. 45.

[3] El 2 de agosto de 2011, los medios de comunicación se hace eco del estudio de un grupo de investigadores de la universidad Carnegie Mellon de EEUU que demuestran que con un teléfono móvil (dotado de cámara fotográfica y conexión a Internet) es posible identificar a una persona en

permiten la captación de imágenes como la videovigilancia y respecto de los que existe mayor consenso respecto del carácter grave de su incidencia en el derecho a la intimidad, es pretensión de este trabajo ocuparse principalmente de aquellos medios que con carácter específico están destinados a la localización y seguimiento, y su incidencia en el derecho a la intimidad.

Irremediablemente, los juristas están llamados a conocer y comprender, aún de forma somera, el funcionamiento básico y los potenciales de aquellas tecnologías que pueden suponer una agresión a los derechos de las personas, como requisito previo a la búsqueda del necesario equilibrio que debe establecerse entre el bien jurídico al que sirve el uso de la tecnología de vigilancia y el que se verá agredido por la misma. Por ese motivo, este trabajo se presenta como un estudio híbrido que analiza el derecho a la intimidad, sus límites y posibilidad de injerencia desde una perspectiva jurídica así como desde la descripción de los medios técnicos que permiten la intervención sobre el derecho.

II. APROXIMACIÓN AL DERECHO A LA INTIMIDAD Y SU LIMITACIÓN

En un análisis como el que se pretende, antes de abordar los pormenores de cualquier tecnología de geolocalización, se hace precisa una visión previa —aún somera— del derecho fundamental a la intimidad, recogido en el artículo 18 de nuestra Carta Magna, pues es sobre este derecho en el que incidirán mayormente las medidas de vigilancia y control que efectúen los miembros de las Fuerzas de Seguridad en su actuación como policía judicial al aplicar técnicas de control de localización y vigilancia, bien sea directamente o valiéndose de medios tecnológicos.

Los derechos y libertades de la esfera privada, junto con los derechos de ámbito personal —de los que son su necesaria proyección— aseguran a los individuos un indispensable campo de libertad y autonomía, impidiendo las intromisiones no deseadas. Así, forman parte de los derechos de la personalidad, y atribuyen por tanto un poder jurídico a las personas con el fin de proteger sus cualidades más esenciales y definidoras del ser humano. Todos ellos son irrenunciables, intransmisibles, imprescriptibles, inalienables e inembargables, sin perjuicio de los supuestos de autorización o consentimiento[4].

Desde estas premisas, los derechos y libertades de la esfera privada se reconducen, en terminología de la doctrina alemana de los derechos públicos subjetivos, al *status libertatis*, o según la doctrina anglosajona, se consideran derechos que garantizan una esfera de libertad negativa, ya que protegen un espacio de intimidad que

el acto, fotografiándola y, mediante una herramienta informática, cruzarlas con las existentes en las bases de datos fotográficas de las redes sociales como facebook.

4 STC 214/1991.

se quiere preservar frente a las intromisiones externas, tanto poderes públicos como por parte de terceros privados que se pudieran producir sin previa autorización.

Hay consenso al considerar que es la obra "*The right to privacy*" de BRANDEIS y WARREN[5] la que sienta las bases de la doctrina alemana de las esferas o círculos concéntricos. En palabras del profesor DESANTES[6], la intimidad es "aquello que queda de la piel del hombre hacia dentro", como son los sentimientos, apetencias, inclinaciones, ideas, etc. Según la teoría de las esferas, la más interna constituye lo íntimo, a continuación la esfera de lo familiar y por último la esfera de lo público, en el entendimiento que los contornos de cada esfera dependerán de cada persona, atendiendo a su propia individualidad y percepción de lo que para él es íntimo o lo que no le importa que sea público.

Para el Tribunal Constitucional "*el atributo más importante de la intimidad, como núcleo de la personalidad, es la facultad de exclusión de los demás, de abstención de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos intrusiva, como a la divulgación ilegítima de estos datos*"[7].

A nuestro juicio, en la configuración del derecho a la intimidad personal, cada día cobra más relevancia la *teoría del mosaico*, como necesario complemento a la concepción clásica de las esferas concéntricas, si en verdad queremos hacer frente a la nueva realidad a la que se enfrenta su protección. MADRID CONESA[8] estima lo privado y lo público como conceptos relativos[9] en función de quién sea el otro sujeto en la relación informativa, y en segundo lugar, que existen datos en principio irrelevantes desde el punto de vista del derecho a la intimidad y que, sin embargo, en conexión con otros, quizá también irrelevantes, pueden servir para hacer totalmente transparente la personalidad de una persona "*al igual que ocurre con las pe-*

5 WARREN D.S. Y BRANDEIS D.L.:"The right to privacy" publicado en el nº 5, volumen IV de la Harvard Law Review en 1890. Traducción española titulada El derecho a la intimidad publicada por Civitas, Madrid, 1996. Según los autores "gradualmente se ha ido ensanchando el alcance de esos derechos, y ahora el derecho a la vida ha llegado a significar el derecho a disfrutar la vida, el derecho a ser dejado en paz; el derecho a la libertad asegura el ejercicio de amplios privilegios civiles; y el término 'propiedad' ha llegado a comprender toda forma de posesión —tanto tangible como intangible—".

6 DESANTES GUANTER, J.M. Y SORIA, C.: Los límites de la información, Asociación de la Prensa de Madrid, Madrid, 1991, pág. 109.

7 STC 142/1993, de 22 de abril.

8 Vid. nº 2.

9 No es pacífica esta opinión, no faltando quienes afirman no poder compartir la idea de que lo privado sea relativo al seguir existiendo aspectos que objetiva y sustancialmente, son íntimos o privados y, en consecuencia, son merecedores de tutela. Quizá lo que es relativo es lo público, con la consecuencia de que hay ciertos datos públicos que pueden tener una trascendencia para la intimidad si se conectan entre sí. Se produciría una suerte de metamorfosis que convierte los datos públicos en privados o íntimos. Lo cierto es que la teoría del mosaico permite dar cabida a los problemas que suscita la intimidad informática.

queñas piedras que forman los mosaicos, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado".

Debemos admitir que el concepto de derecho a la intimidad ni es ni puede ser cerrado debido a su componente subjetivo, tanto desde el aspecto individual como del colectivo o de los grupos sociales, en función de elementos como la educación.

El análisis jurisprudencial del derecho a la intimidad nos lleva a distinguir dos vertientes: la objetiva y la subjetiva.

La primera aproximación al concepto objetivo de intimidad nos la ofrece la definición de la Real Academia de la Lengua Española, como la *"zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia"*. Este concepto objetivo se identifica con la protección de un ámbito concreto de la personalidad del individuo, de su dignidad como persona.

La vertiente subjetiva del concepto se identifica, especialmente a los efectos de nuestro análisis, con el derecho a la autodeterminación informativa. Nuestro Tribunal Constitucional, en sentencia 110/1984 afirmó que *"los distintos apartados del artículo 18 de la Constitución tienen como finalidad principal el respeto a un ámbito de vida privada, personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de la tecnología, salvo autorización del interesado"*. Es lo que se ha venido a denominar *"derecho de autodeterminación informativa"*. El precedente moderno lo encontramos en el Tribunal Constitucional de Alemania que, en 1983, la definió como *"la facultad del individuo derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida"*[10]. Es el individuo el que determina lo que debe o no quedar reservado al conocimiento de terceros. El concepto subjetivo responde a la *libertad de disposición* de la información relativa a lo más íntimo, como la capacidad de cada persona de controlar lo que de ella se pueda conocer.

Esta nueva concepción de la intimidad como derecho a la autodeterminación informativa surge ante la falta de capacidad de los instrumentos de tutela para afrontar la potencial incidencia que en la intimidad producen los medios tecnológicos (en especial la informática). Este derecho, —hoy fundamental— tras un tibio reconocimiento doctrinal, ha sido incorporado a ordenamiento jurídico así como a la jurisprudencia constitucional[11]. También a nivel europeo[12]

[10] Sentencia del Tribunal Constitucional Federal alemán sobre la Ley del Censo de Población de 15 de diciembre de 1983, sentó las bases del derecho a la autodeterminación informativa, el derecho de cada persona a controlar las informaciones y datos que a ella se refieren. Cabe señalar que la Ley Fundamental de Bonn no contiene ninguna referencia literal a este derecho.

[11] STCS 290/2000 y 292/2000.

[12] La Carta de Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000, en su artículo 8 "Toda persona tiene derecho a la protección de los datos de carácter personal que

En conclusión, como afirma REBOLLO DELGADO, *"cabe entender el derecho a la intimidad como la protección de la autorrealización del individuo"*, *"la intimidad es el elemento de desconexión social"*[13], o de una forma coloquial podríamos decir con LUCAS MURILLO[14] que el derecho a la intimidad es *"el derecho a que nos dejen en paz"*.

El potencial de los nuevos medios tecnológicos de la sociedad de la información han activado las alarmas a favor de la defensa de una necesaria esfera de privacidad, defensa de una intensidad desconocida en épocas pasadas. Según LUCAS MURILLO se debe a que la vida privada se asocia a la propia libertad que ha de desenvolverse en nuevas formas de masificación social fruto de las modernas formas de urbanización, con el añadido de medios tecnológicos que permiten la difusión de información casi sin limitación. *"Excluir parcelas de nuestra vida del conocimiento ajeno se ha convertido en una forma de ser libres"*, apunta MURILLO. El bien jurídico que representa la necesidad básica de libertad y consecuente desempeño de cierta esfera de nuestra actuación al margen del conocimiento de terceros es a lo que llamamos intimidad.

El derecho a la intimidad, sin embargo, no constituye un derecho absoluto sino que se encuentra limitado por otros derechos y bienes jurídicos de relevancia constitucional, como es el mantenimiento de la seguridad ciudadana, que tiende a preservar los derechos de los demás ciudadanos. La Constitución no prevé de forma expresa la posibilidad del sacrificio legítimo de los derechos del artículo 18.1 *(derecho al honor, a la intimidad personal y familiar y a la propia imagen)* como, al contrario, sí lo hace respecto de la inviolabilidad de domicilio o secreto de las comunicaciones. Sin embargo, esto no puede significar que estemos ante un derecho que no permite ningún tipo de restricción, debiendo ceder ante razones justificadas convenientemente previstas por la ley. Es el caso, como sentencia el Tribunal Constitucional, de la protección de los derechos y libertades de los ciudadanos y la preservación de la seguridad ciudadana.

> *A las citadas competencias hace igualmente referencia el escrito de alegaciones de la representación del Gobierno Vasco, insistiendo en la labor de prevención de desórdenes y de preservación de aquellos derechos y libertades que llevó a cabo la policía en el presente supuesto. Estos son, efectivamente, bienes constitucionalmente relevantes, que, como hemos afirmado en múltiples resoluciones (por todas STC 91/1983, fundamento jurídico 3.°), pueden dentro de ciertos límites restringir el ejercicio de los derechos y libertades constitucionales y cuya preservación está constitucionalmente atribuida a las*

la conciernan. Esos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley.

[13] REBOLLO DELGADO, ., "Derechos fundamentales y protección de datos", Dykinson. Madrid, 2004, pág. 40.

[14] LUCAS MURILLO DE LA CUEVA, P. "El derecho a la autodeterminación informativa y la protección de datos personales" San Sebastián, 2007. pág. 45.

Fuerzas y Cuerpos de Seguridad del Estado ex art. 104.1 CE que explícitamente establece que "tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana".
(...)
En suma, a la vista de estos datos, puede concluirse que en el presente caso concurría la existencia de un bien constitucionalmente legítimo como es la protección de los derechos y libertades de los ciudadanos y la preservación de la seguridad ciudadana que, en principio, podía justificar la adopción de una medida de control preventivo. (STC 37/1989)

De nuestra configuración constitucional no puede deducirse, siguiendo a BUENO GALLARDO[15], que exista intimidad alguna que no sea susceptible de afectación por los poderes públicos, pues incluso la intimidad domiciliaria puede ser quebrantada cuando existen motivos suficientes, con la supervisión del juez. Nos encontramos ante la colisión un derecho fundamental, la intimidad personal, con el derecho a la seguridad pública[16]. Este último derecho no tiene carácter de derecho fundamental, sin embargo vemos con frecuencia como el primero cede ante el segundo. Ahora bien, no podemos desconocer que el derecho a la seguridad entronca con otros derechos fundamentales como es la inexcusable salvaguarda de la vida, soporte básico del resto de derechos.

15 BUENO GALLARDO, E.: "La configuración constitucional del derecho a la intimidad" Centro de Estudios Constitucionales, Madrid, 2009.

16 La doctrina del Tribunal Constitucional ha sido titubeante a la hora de definir qué entiende por seguridad ciudadana, pues en ocasiones las considera integradas (STC 104/1989) y en otras de forma independiente (STC 325/1994). Llama la atención que en esta última sentencia, el inciso "*sin olvidar a la policía judicial para la averiguación del delito y descubrimiento del delincuente*"
STC 104/1989, la seguridad pública, entendido como "*actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad y el orden ciudadano, según pusimos de relieve en las SSTC 33/1982, 117/1984, 123/1984 y 59/1985, engloba, como se deduce de estos pronunciamientos, un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido*".
STC 325/94, "*... [La seguridad ciudadana] a su vez, aparece conectada a la tercera especie, la seguridad pública (art. 149.1.29 C.E.) también llamada ciudadana, como equivalente a la tranquilidad en la calle. En definitiva, tal seguridad se bautizó ya en el pasado siglo con la rúbrica del 'orden público', que era concebido como la situación de normalidad en que se mantiene y vive un Estado, cuando se desarrollan las diversas actividades colectivas sin que se produzcan perturbaciones o conflictos. En definitiva, el normal funcionamiento de las instituciones y el libre y pacífico ejercicio de los derechos individuales según lo definía la Ley homónima de 28 de julio de 1933, durante la Segunda República. Tal era el sustrato, también, de la que con la misma rúbrica y finalidades había promulgado el 23 de abril de 1870, bajo la Constitución de 1869. En la nuestra de 1978 se encuentran otras alusiones a la seguridad ciudadana desde la perspectiva de quienes han de garantizarla, así como de proteger el libre ejercicio de los derechos y libertades, misión privativa de las Fuerzas y Cuerpos correspondientes (art. 104 C.E.), sin olvidar a la policía judicial para la averiguación del delito y el descubrimiento del delincuente (art. 126 C.E.) normas constitucionales que desarrolla la Ley Orgánica 2/1986, de 13 de marzo, reguladora de los servidores de esa función*".

No debe perderse el horizonte que persigue, en este caso, una posible injerencia en el derecho de la intimidad, pues para que se produzca una sentencia condenatoria (por un hecho penal) es preciso que se haya desvirtuado, mediante la actividad probatoria, la presunción de inocencia[17]. En el desarrollo de la actividad encaminada a conseguir los elementos que permitan probar la existencia del hecho delictivo y su participación en el mismo, la policía judicial puede haber utilizado medios de investigación tecnológicos, como aquellos que permiten la captación de imágenes con un alto potencial de intromisión en la esfera de privacidad y, en consecuencia, en un derecho fundamental como el que nos ocupa. Es por ello que para no incurrir en la prueba ilícita, la actividad que pretende obtener el material probatorio ha de cumplir los unos presupuestos básicos de habilitación legal, finalidad legítima, intervención judicial y proporcionalidad[18] que analizaremos tras un resumido estudio de los medios técnicos de seguimiento más habituales.

III. MEDIDOS Y TÉCNICAS DE LOCALIZACIÓN Y SEGUIMIENTO

Como venimos anticipando, las Fuerzas de Seguridad y el servicio estatal de inteligencia, en España el Centro Nacional de Inteligencia (CNI)[19], utilizan diversas tecnologías para localizar y seguir —en el espacio— a sus objetivos, en favor de la protección de derechos y libertades públicas y de la seguridad ciudadana.

La utilización de medios técnicos por parte de las Fuerzas de Seguridad obedece a la necesidad de afrontar nuevas situaciones creadas especialmente por la delincuencia organizada. Estas organizaciones se valen de las últimas tecnologías en el desempeño de su actividad delictiva y, en muchas ocasiones, cuentan con más y mejores medios que las Fuerzas de Seguridad. Es por ello que el Poder Público tiene la necesidad de nivelar el desequilibrio que produce la diferencia entre los medios de unos y otros, tecnificando los mecanismos de investigación, lo por permite abordar mayor número de investigaciones sirviéndose de menores recursos humanos. Un operativo de seguimiento por medios tecnológicos puede ser controlado por una

17 ASENCIO MELLADO, *Prueba prohibida y prueba preconstituida* ob. cit, págs. 41-43

18 Estos presupuestos son analizados con mayor detalle en epígrafe VI de este trabajo.

19 Es necesario precisar la diferencia cualitativa que, en la obtención de información, existe entre las Fuerzas de Seguridad y el CNI, pues mientras los primeros han de orientar la obtención hacia la calidad, pues el dato obtenido tiene vocación procesal, lo que conlleva una revisión judicial de la metodología de obtención que lo puede hacer inútil, y por ende, todo lo que dependa de él (*doctrina del árbol envenenado*), los servicios de inteligencia, sin perjuicio de la pretendida calidad, tienen por objetivo la cantidad y su posterior análisis, pese a que unos y otros puedan utilizar los mismos medios técnicos. La Doctrina del fruto del árbol envenenado, con origen en la jurisprudencia norteamericana, (the fruit of the poisonous tree) Caso Nardone vs US (302 US 379, 1939), hace referencia a una metáfora legal para describir la invalidez de la evidencia recolectada con ayuda de información obtenida ilegalmente.

sola persona mientras que su materialización mediante métodos tradicionales consume un alto número de personas, incluso de medios materiales como vehículos.

Entre los medios de seguimiento y vigilancia encontramos:

1. *Balizas (dispositivos de control remoto)*

Estos artilugios han experimentado una trascendental evolución en los últimos años, permitiendo el seguimiento no sólo de personas, sino de objetos como vehículos, embarcaciones, obras de arte, etc.

Podemos clasificarlos en función de la tecnología de que se valen:

- Sistemas de señal por radio, entre los que destacamos:
  - Sistemas específicos de apoyo al operativo de seguimiento que se basa en el análisis de la intensidad y dirección de la señal, localizando el objeto de localización en referencia al operativo de seguimiento sobre un mismo sistema.
  - Utilización de un despliegue de antenas que mediante triangulación de la señal permite obtener una ubicación aproximada del objetivo.
- GPS. Los equipos que integran GPS recogen la señal emitida por varios satélites que permite, por su posición relativa, ubicar con un mínimo error el dispositivo que integra GPS. Es una tecnología popularizada ya que es la que integran los navegadores de los vehículos y es utilizada para el control de flotas de vehículos, en los dispositivos antirrobo en vehículos o las polémicas pulseras anti-maltrato colocadas sobre condenados por violencia de género. Debido al carácter militar del sistema GPS, el Departamento de Defensa de los EE. UU. se reservaba la posibilidad de incluir un cierto grado de error aleatorio, que podía variar de los 15 a los 100 metros, sin embargo la llamada disponibilidad selectiva (S/A)[20] fue eliminada el 2 de mayo de 2000. Aunque actualmente no aplique tal error inducido, la precisión intrínseca del sistema GPS depende del número de satélites visibles en un momento y posición determinados. Con un elevado número de satélites siendo captados (7, 8 o 9 satélites), y si éstos tienen dispersión adecuada, pueden obtenerse precisiones inferiores a 2,5 metros si se activa el sistema GPS Diferencial (DGPS) que proporciona corrección sobre los datos recibidos de los satélites GPS. Estas correcciones, una vez aplicadas, proporcionan mayor precisión a la localización. Existen varias formas de proporcionar corrección DGPS. Las más usadas son[21]:
  - El llamado SBAS[22] la precisión mejora siendo inferior a un metro en el 97% de los casos[23].
  - Recepción de señal de radio, como el RDS en una emisora FM o el célebre Wi-Fi.
  - Correcciones descargadas por Internet con conexión inalámbrica.
- Satélites independientes. Se trata de satélites destinados al control de un espacio determinado y concreto, frente a la cobertura total del GPS. En relación al seguimiento, tienen por finalidad el control de objetivos que se mueven a baja velocidad y cuyo seguimiento ha de ser mantenido durante un largo periodo, como es el caso de las largas travesías oceánicas de embarcaciones. Este sistema permite obtener la señal de localización a través de telefonía vía satélite, dado que es posible que el objetivo se esté moviendo por zonas (como altamar) por las que no existe ningún otro medio (radio, gsm, etc.) que permita enviar la posición al operativo de control.
- Tecnología GSM. Se trata de la utilización del despliegue del sistema de repetidores para telefonía móvil. Se basa en la recepción de la señal por el repetidor de cada celda, y respecto de la que se emplea técnicas básicas de localización como la trilateración, triangulación y multilateración[24].
- Dispositivos de descarga de archivos *log*[25]. Sistema que acumula las distintas ubicaciones del dispositivo de localización GPS o terminal móvil, pero que no persigue la localización en tiempo real sino que descarga la información

[20] La conocida como Disponibilidad Selectiva (S/A en su acrónimo inglés) es una degradación intencionada de la seña GPS con el fin de evitar la excesiva precisión de los receptores GPS comerciales modernos.

[21] III Congreso Virtual Intervisual sobre la autonomía personal de personas con ceguera o deficiencia visual. Octubre 2005.
http://juntadeandalucia.es/averroes/caidv/interdvisual/iiicv/gps_ay_orientacion_pc.pdf

[22] SBAS, abreviatura inglesa de *Satellite Based Augmentation System* (Sistema de Aumentación Basado en Satélites), es un sistema de corrección de las señales que los Sistemas Globales de Navegación por Satélite (GNSS) transmiten al receptor GPS del usuario. Los sistemas SBAS mejoran el posicionamiento horizontal y vertical del receptor y dan información sobre la calidad de las señales. Aunque inicialmente fue desarrollado para dar una precisión mayor a la navegación aérea, cada vez se está generalizando más su uso en otro tipo de actividades que requieren de un uso sensible de la señal GPS.

[23] http://es.wikipedia.org/wiki/Sistema_de_posicionamiento_global

[24] Vid. nº 31

[25] Un *log* es un registro de eventos durante un rango de tiempo en particular. En el campo de la informática tiene la finalidad de registrar los datos e informaciones sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación informática. Entre los datos que guarda los ficheros log de nuestros terminales móviles, relativos a la localización, podemos destacar:
MCC (Mobile Country Code): Es un dato que hace referencia al país en el que se encuentra el usuario en el instante de la medición (o para ser mas exactos, el país en el que se ubica la estación base a la que el usuario está asociado en ese instante).

en un momento posterior. Por ejemplo el fichero LOCI se aloja en la tarjeta SIM de los teléfonos móviles conteniendo el LAI que nos indicará en qué área ha estado el teléfono la última vez que operó.

2. *Interceptación telefónica mediante software o hardware*

En una sociedad cada vez más tecnificada se hace necesario, en el ámbito de la investigación policial-procesal, la intromisión en los sistemas automáticos de información, del mismo modo que en el ámbito convencional existe la figura del agente encubierto que se infiltra en las organizaciones criminales para obtener información.

En esta modalidad podemos incluir el *hacking o cracking legal* que no son otras actividades que aquellas que permiten acceder a los sistemas de informáticos que usan los investigados, quebrando sus sistemas de seguridad y, en muchos casos, colocando en esos sistemas "*programas infiltrados*" que permitirán a los investigadores acceder, observar y obtener copia de los contenidos (documentos, comunicaciones, etc.)

En este ámbito podemos hablar de la posibilidad de duplicar o *clonar* un terminal telefónico. Esta actuación puede efectuarse de dos modos. Mediante la intervención física e instalación de un chip o la instalación remota de software que permite controlar toda la actividad del teléfono original como tener conocimiento de la BTS a través de la que actúa y, en consecuencia de su ubicación. Esta herramienta permite incluso la activación del micrófono[26] del teléfono aunque se encuentre apagado[27].

MNC (Mobile Network Code): Identificador del operador de red. Es único para cada operador dentro de su país, lo que quiere decir que mismos identificadores pueden repetirse fuera del territorio nacional.
LAC (Location Area Code): Código identificador de área. A aquellas regiones con cobertura GSM se les asigna un código LAC único dentro de cada país.
Cell ID: Identificador de célula. Es un número que identifica de forma unívoca a una célula (celda) dentro de un territorio nacional.
Células vecinas: El teléfono móvil almacena por orden las 7 celdas más cercanas al terminal. Dicho criterio de cercanía se basa en la potencia de la señal recibida por cada BS.

26 Funcionalidades como la citada son cada vez más conocidas, especialmente en el mundo de los hackers. Un sencillo paseo por Internet nos da muestra de lo fácil que resulta conseguir software espía y productos comerciales que permiten controlar la localización de un objeto mediante la combinación GPS y GSM (UMTS), con la incorporación de dispositivos de actuación remota como micrófono que nos permite oír en tiempo real. A modo de ejemplo véase "Localizador GPS.es", http://www.localizadorgps.es/localizador_gps_para_objetos.asp

27 Llamas Fernández, M Y Gordillo Luque, Jm. "Medios Técnicos de Vigilancia" en la obra "Los nuevos medios de investigación en el proceso penal. Especial referencia a la Tecnovigilancia". *Cuardernos de Derecho Judicial*, Madrid, 2007, pág. 237.

3. *Intervención de comunicaciones vía satélite*

La comunicación vía satélite suele ser utilizada en aquellas zonas que no disponen de la cobertura de telefonía convencional, como alta mar. Para que la comunicación por esta vía pueda establecerse es preciso que el satélite conozca la ubicación geográfica del terminal a través del que se efectúa la comunicación.

4. *Vigilancia a través del Sistema de telefonía móvil (GSM-UTMS) Sistema de intervención telefónica SITEL*

Desde hace algunos años se venía localizando la ubicación de teléfonos móviles cuando estos entablaban comunicación. De este sistema se valían especialmente los servicios de emergencia cuando recibían una llamada de auxilio. Se trata de localización activa. Sin embargo ahora nos encontramos con la posibilidad de que la localización se produzca sin que sea necesario entablar comunicación, permitiendo el seguimiento mediante una técnica pasiva, aunque es preciso reseñar que el terminal debe estar encendido; sin perjuicio de que puedan existir mecanismos para activar el teléfono sin conocimiento del portador[28] o la introducción de software que permita hacer creer al usuario que está apagado cuando en realidad sigue operativo.

En cierto modo su fundamento ha sido referido al hablar de las balizas, con la diferencia de que en este caso la "*baliza*", en lugar de ser un artilugio que colocan los equipos de investigación, es el propio terminal telefónico que porta el objetivo, ya que la localización y seguimiento se realiza a través del sistema de telefonía móvil.

Al hablar de sistema de telefonía, aunque sea móvil, es fácil dejarse arrastrar por las tradicionales interceptaciones de comunicaciones y pensar que estamos ante eso, ante la intervención de una comunicación. Sin embargo, la localización a través del sistema de telefonía puede producirse aunque no se realice comunicación telefónica alguna, por cuanto en términos estrictos no estaremos ante una intervención que precisa autorización judicial por interferir sobre el secreto a las comunicaciones[29] sino, ante una localización por un medio tecnológico que permite la ubicación de un terminal telefónico, del mismo modo que se hace con una baliza, con la importante peculiaridad, como se ha dicho, que en este caso las funciones de baliza las hace el propio terminal telefónico que porta el objetivo.

La red de telefonía móvil es un sistema de comunicación en el que se combinan una serie de estaciones transmisoras-receptoras de radio (BTS) y una serie de centrales telefónicas de conmutación que posibilitan la comunicación entre terminales telefónicos móviles, o entre éstos y la red fija de telefonía.

---

28 Vid. nº 22

29 Artículo 18.3 de la Constitución Española. "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".

Su funcionamiento se basa, principalmente, en la actuación bajo un repetidor (BTS) concreto que nos indicará celda[30] o célula de ubicación. Es frecuente hablar de teléfono celular al referirse al teléfono móvil y ello se debe a que las estaciones base, que enlazan vía radio los teléfonos móviles con los controladores de estaciones base, están dispuestas en forma de una malla, formando células o celdas, a modo de panel de abejas. Así, cada estación base está situada en un nudo de estas células y tiene asignado un grupo de frecuencias de transmisión y recepción propio. La suma de equipos que con capacidad de medir la dirección de la señal, su intensidad, y tiempo de respuesta, permiten permite ofrecer una ubicación aproximada del terminal.

La red de telefonía móvil actual es una red digital. En esta red la comunicación se realiza mediante señales digitales, lo que permite optimizar tanto el aprovechamiento de las bandas de radiofrecuencia como la calidad de la transmisión. El estándar de transmisión es el GSM, y UMTS en la tercera generación.

La localización GSM es un servicio ofrecido por las empresas operadoras de telefonía móvil que permite determinar, con una cierta precisión, donde se encuentra físicamente un terminal móvil determinado. Se emplean varios técnicas y métodos[31]

30 Ámbito de cobertura de un repetidor

31 Resulta de interés, describir, aún de forma somera, los métodos y técnicas más elementales que permiten, tras el tratamiento de unos datos básicos (información primaria), obtener otros de mayor precisión en relación a la geolocalización de un terminal telefónico:
Triangulación: Esta técnica hace uso de varios nodos fijos (puntos de conexión) cuya posición es conocida. Cada nodo fijo ha de ser capaz de determinar la dirección (ángulo) en la que se encuentra el punto a localizar. Se emplean antenas direccionales, capaces de captar las ondas que se emiten en puntos distantes siempre en la dirección a la que se oriente dicha antena. Si captamos con una antena direccional la señal que emite el teléfono móvil a localizar, sabremos la dirección sobre la que se encuentra respecto al nodo de referencia, aunque no podremos determinar por este método la distancia a la que se encuentra que habrá que calcular mediante un método complementario. Para ello se emplea una segunda antena direccional ubicada a una distancia conocida del primer nodo, el que captó la dirección de la señal. Esta segunda antena determina de nuevo la dirección relativa sobre la que se encuentra el punto a localizar. Conociendo las dos direcciones relativas a ambos nodos en las que se encuentra el terminal telefónico a posicionar podemos trazar dos rectas (con origen en dichos nodos) que interseccionarían en el emisor (terminal móvil). Sendas rectas junto con la que une los dos nodos que intervienen en el proceso conforman los lados de un triángulo. La distancia entre los nodos es un parámetro conocido, por lo que determina de por sí la longitud de uno de los lados del triángulo. Se conocen también los ángulos contiguos a dicho lado, por lo que aplicando simples operaciones trigonométricas se es capaz de calcular la distancia de los nodos al punto incógnita y esto implica automáticamente la posibilidad de posicionar en el plano la estación móvil objetivo. También podemos realizar una triangulación en vez de con una antena direccional, con un conjunto de antenas capaces de determinar diferentes TDOAs junto con un AoA para cada antena y así estimar las direcciones.
Trilateración: A diferencia de la triangulación (la cual usa ángulos), la trilateración emplea tan sólo distancias para estimar la posición de un terminal móvil en un plano bidimensional. Para llevar a cabo esta tarea, se calcula la distancia a la que se encuentra un terminal móvil por parte de al menos 3 antenas, las cuales trazan circunferencias sobre las que se encuentra el punto de medición. Dos circunferencias que interseccionan lo hacen en uno o dos puntos; un tercer nodo describe una tercera circunferencia que determina el punto donde se encuentra el terminal móvil.
Multilateración: La multilateración, también llamada posicionamiento hiperbólico, es una técnica que emplea la magnitud TDOA para el posicionamiento tridimensional de una estación móvil mediante un mínimo de 4 antenas. Conociendo la posición de 2 antenas (las cuales ya no necesitan ser unidireccionales) y conociendo el TDOA de una señal proveniente de la MS a localizar, el problema de búsqueda del punto emisor se reduce a localizar al mismo en el interior de un hiperboloide de dos hojas. Añadiendo un tercer nodo de medición se obtiene una nueva diferencia de tiempos de llegada, lo que genera un nuevo hiperboloide que intersecciona con el anterior, reduciendo el problema a una curva en la superficie de una de las dos hojas del hiperboloide. Si añadimos una cuarta antena, obtenemos un nuevo TDOA y generamos un nuevo hiperboloide. Dicho hiperboloide intersecciona con los otros dos (o con la curva generada por la intersección de los dos primeros hiperboloides) en un único punto común, que es el punto a determinar. En este caso, se da también la coordenada de altura del punto de medición.
TA (Timing Advance): Procedimiento por el cual una estación base es capaz de calcular la distancia a la que se encuentra un terminal del propio nodo (o viceversa). Para ello se miden los retardos de propagación de las señales radioeléctricas que intervienen en la comunicación entre BTS y terminal. Sabiendo que dichas señales viajan a una velocidad cercana a la de la luz podemos estimar (con mala precisión) dicha distancia, para trazar una circunferencia sobre la cual se ubicaría el MS.
Existen otros métodos para mejorar la precisión: TDOA (Time Difference Of Arrival): TOA (Time Of Arrival), AoA (Angle of Arrival), CGI (Cell Global Identit,), CGI-TA, A-GPS (Assisted Global Positioning System) Criptolab. Facultad de Informática de la Universidad Politécnica de Madrid
http://www.kriptopolis.org/geoposicionamiento-gsm-1

para la localización GSM. El más simple se basa en el CELL ID o *identificador de celda*. El sistema conoce la celda en la que se encuentra el teléfono móvil y por tanto puede estimar su posición. Otros métodos emplean el sistema GSM en combinación o asistido por GPS mejorando sustancialmente la precisión en la localización.

En cuanto a la tecnología UMTS[32], es el sistema de telecomunicaciones móviles de tercera generación, que evoluciona desde GSM y está teniendo un papel primordial en las telecomunicaciones multimedia inalámbricas de alta calidad.

Venimos manteniendo que no es necesario que se establezca una comunicación en el sentido formal al que nos referimos al hablar de intervención de las comunicaciones. Sin embargo, aunque no hablemos, existe un constante "diálogo técnico" entre el terminal telefónico y la antena (BTS) bajo cuyo ámbito de cobertura se encuentra. En ese diálogo se generan datos a los que nos referimos como datos de localización "distintos a los del tráfico"[33]. Cualquier teléfono, por el mero hecho de estar encendidos *"stand by"* deja un rastro. Ese rastro puede convertirse en dato de carácter personal[34] en el momento que sea vinculado a una persona concreta

32 UMTS: Universal Mobile Telecommunications System-Sistema Universal de Telecomunicaciones Móviles, estándar de telefonía móvil de banda ancha. Se trata de un sistema de tercera generación que permite la conexión a Internet.

33 Directiva 2002/58/CE. Art. 9

34 Dato de carácter personal es cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables,

y desde ese momento ponerse en íntima relación con el derecho a la intimidad. Hablamos por tanto de la posibilidad de ubicar, de forma constante, con independencia de que se produzca o no comunicación —en sentido convencional— a un objeto, y su posibilidad de atribuir la localización y el movimiento a su portador. Esta localización constante crea un nuevo riesgo, el de la construcción de perfiles de comportamiento y de movimiento que no se debe tanto a la mera localización puntual sino a que ésta se prolongue en el tiempo.

Estos datos permiten, de forma derivada, obtener otros productos "cualificados" que han venido a denominarse *servicios de valor añadido*[35], *en nuestro caso "servicios basados en la localización" —Localiton Bases Services, LBS—*. Se trata de los servicios basados en la localización y que no sólo se basan en telefonía móvil sino que se complementan con GPS y otras tecnologías como Wi-Fi.

En este epígrafe es inevitable hacer una referencia al famoso Sistema de Intervención Telefónica (SITEL) en cuanto a su capacidad para localizar la ubicación de los terminales a través de los que se establece la comunicación. SITEL no es una nueva tecnología de interceptación, sino un sistema informático de gestión de la información y datos que se generan tanto en las intervención de comunicaciones como en el "diálogo técnico" entre terminal y BTS del operador telefónico bajo cuya cobertura se encuentra. SITEL sustituye a la antigua grabadora y a la libreta de notas del investigador policial. Los datos, en formato digital, se vuelcan es este sistema. SITEL no aporta un plus en cuanto a las posibilidades de interceptar y localizar un terminal al margen de las tecnologías descritas. Sin embargo, no podemos despreciar el riesgo que esta herramienta puede suponer al posibilitar un actual y futuro tratamiento masivo de datos que permite la tecnología digital frente a una clásica grabadora analógica, como lo supuso el cambio cualitativo entre un fichero en papel y un fichero informatizado.

En concreto SITEL plantea cuestiones comunes a otros medios de prueba obtenidos por medios tecnológicos, como es la garantía de su autenticidad, integridad y no alteración de los datos que, en soporte digital, se pueden obtener a través del mismo. Sin embargo, ahora, por la finalidad de este estudio, nos basta centrarnos en el potencial de ubicar geográficamente un terminal telefónico, aún con cierto

según la definición del *artículo 5 del Reglamento de la Ley de Protección de Datos de Carácter Personal*. Los datos que nos llevan a la ubicación de un objeto y sus desplazamientos, siempre que se puedan atribuir a una persona identificada o identificable constituyen dato de carácter personal. A esa conclusión se llega en informes de la Agencia Española de Protección de Datos, entre otros el informe nº 193/2008 (relativo a datos emitidos por GPS instalados en vehículos).

35 Según el artículo 64.e del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de usuarios, se trata de los "servicios con valor añadido", aquellos que requieren el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vaya más allá de lo necesario para la transmisión de una comunicación o su facturación.

margen de error, y mantener ese control en el tiempo, sin que para ello sea preciso entablar conversación alguna a través del terminal telefónico.

5. Wi-Fi. (Localización a través de puntos de acceso)

Wi-Fi[36] es nueva fuente de información relativa a geolocalización mediante el uso de mapas de puntos de acceso a las redes WiFi. La tecnología es similar a la utilización de estaciones base de la red de telefonía. Ambos se basan en una identificación única, (desde la estación base o punto de acceso Wi-Fi), que puede ser detectado por un dispositivo móvil, y se envía a un servicio que goza de una ubicación conocida para cada identificador único.

El identificador único para cada punto de acceso WiFi es su dirección MAC[37]. Una dirección MAC es un identificador único asignado a una interfaz de red y generalmente se registra en el hardware, tales como chips de memoria y/o tarjetas de red en computadoras, teléfonos, ordenadores portátiles o puntos de acceso.

La razón de que los puntos de acceso Wi-Fi se puede utilizar como una fuente de información de geolocalización se debe a que continuamente anuncian su existencia. La mayoría de los puntos de acceso a internet de banda ancha tienen, por defecto, antena WiFi. La configuración predeterminada de la mayoría de los puntos de acceso de uso común en Europa es que esta conexión es "on", incluso aunque el usuario se conecte a su *modem* o *enrrutador* mediante cable. El punto de acceso a red Wi-Fi transmite continuamente su propia red, nombre y su dirección MAC, incluso si nadie está utilizando la conexión e incluso en el caso el contenido de la comunicación inalámbrica está encriptado[38]. (Cualquiera puede comprobarlo mediante un sencillo escaneo de redes inalámbricas desde su ordenador o teléfono móvil).

Hay dos maneras de recolectar las direcciones MAC de los puntos de acceso WiFi:

36 Wi-Fi: *Wireless Fidelity*-(Fidelidad sin cables), conjunto de estándares del IEEE para redes locales inalámbricas, con velocidad de transmisión de datos de hasta 54 Mbit/s, en las bandas de frecuencia que no requieren licencia. *Wi-Fi Alliance* es la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 8802.11 relacionados a redes inalámbricas de área local. En realidad Wi-Fi es una marca comercial. Se un conjunto de redes que no requieren de cables y que funcionan en base a ciertos protocolos previamente establecidos (Estándares IEEE 802.11) Si bien fue creado para acceder a redes locales inalámbricas, habiéndose convertido en unos de la medios más utilizados para conectarse a internet.

37 MAC: *Media Access Control adress*. Dirección de Control de acceso al medio. Una dirección MAC es un identificador único en el mundo y está representado en notación hexadecimal y conformado por 48 bits. Dicho identificador se asigna a las tarjetas de red de los ordenadores.

38 Los sistemas de encriptamiento son WEP, WPA o WPA2.

1. *Activos*: el envío de solicitudes activas a todos los puntos de acceso Wi-Fi cercanos y la posterior grabación de sus respuestas.
2. *Pasivos*: Se basa en la observación y grabación de los datos intercambiados entre el punto de acceso y los aparatos que con él se relacionan. Este tipo de análisis podría llevar también a la grabación ilegal de los contenidos de las comunicaciones, que serán fácilmente legibles en caso de que el propietario del punto de acceso Wi-Fi no haya efectuado el cifrado de su WiFi.

La ubicación de un punto de acceso Wi-Fi se puede calcular de dos formas diferentes.

1. *De forma estática*: los controladores recogen las direcciones MAC de acceso WiFi escaneando la señal con una antena de la que se conoce la ubicación y respecto de la que se calculará la distancia en función de la fuerza de la señal. Ese almacenamiento masivo de MAC y asignación a lugares determinados puede realizarse recorriendo las calles de una localidad con un vehículo dotado del equipo necesario.
2. *De forma dinámica*: los usuarios de los servicios de geolocalización automáticamente recogen la dirección MAC con sus dispositivos WiFi al usar servicios de localización online, por ejemplo al usar un mapa *on line* para determinar su propia posición. El dispositivo móvil envía toda la información de que dispone al proveedor de servicios de geolocalización, incluyendo dirección MAC, SSID[39] y la intensidad de la señal que permitirá al controlador chequear en su base de datos.

Es importante tener en cuenta que no es necesario que los dispositivos móviles se conecten con los puntos de acceso WiFi para recoger la información, pues la presencia de puntos de acceso es detectada automáticamente y del mismo modo, automáticamente se recogen los datos sobre ellos.

Además, los teléfonos móviles que piden ser geolocalizados no sólo enviar datos de Wi-Fi, sino que suelen enviar cualquier otra información relativa a la ubicación, incluyendo los datos de geoposicionamiento proporcionados por el GPS así como la estación, lo que permite mejorar la base de datos del controlador como la propia localización del terminal. De ese modo se produce se produce una recopilación de información sobre el punto de acceso Wi-Fi de modo descentralizado, sin ser necesariamente los usuarios conscientes de ello.

La localización que permite la red WiFi es un importante complemento en el campo de la geolocalización por funcionar en interiores, allá donde la tecnología GPS flaquea en sus capacidades, en el interior de edificios. En zonas pobladas, es posible determinar la ubicación precisa del punto de acceso, ofreciendo mayor dificultad aquellas muy pobladas donde puede haber confusión entre, por ejemplo, varios pisos del mismo edificio.

En resumen, la geolocalización basada en puntos de acceso Wi-Fi proporciona una rápida y, sobre la base de mediciones continuas, cada vez más precisa la ubicación.

[39] Identificador de red inalámbrica. Es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos.

6. *Localización mediante el control indirecto de datos personales*

Hasta ahora nos hemos aproximado a los medios que utilizan los investigadores para obtener, de forma directa, datos que le permiten localizar en el espacio a sus objetivos pero en multitud de ocasiones, los datos que permiten la geolocalización son obtenidos por un tercero del que serán recabados por el investigador.

Cada día son más las bases de datos que existen, en las que quedará reflejado algún rastro de nuestra actividad y, en consecuencia de nuestros movimientos físicos, de nuestra ubicación.

Así, cuando nos movemos en vehículo, cuando nuestro vehículo es identificado (la matricula del vehículo) al entrar en un parking[40] o con ocasión de una infracción de tráfico, estamos delatando nuestra ubicación. Los datos de la matrícula pueden ser integrados en un fichero automatizado que reflejará lugar y fecha en la que hemos estado. Del mismo modo ocurre cuando nos registramos en un establecimiento hotelero y nuestros datos son incorporados a los ficheros de la Guardia Civil o del Cuerpo Nacional de Policía[41], listas PNR[42], los sistemas de reconocimiento biométrico, la actividad bancaria como el uso de cajeros automáticos, etc. La integración

[40] Se trata de la tecnología informática basada en OCR que permite convertir una imagen (fotografía de la matrícula) en texto y, en consecuencia, su tratamiento en una base de datos automatizada.

[41] La Orden en INT/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos, establece:
Artículo Tercero. Comunicación de datos a las dependencias policiales.
1. Los establecimientos comprendidos en el ámbito de aplicación de la presente Orden deberán comunicar a las dependencias policiales la información contenida en las hojas-registro a que se refiere el apartado anterior, por cualquiera de los siguientes sistemas: (...)
1.4 Mediante transmisión de ficheros vía Internet al Centro de Proceso de Datos de la Dirección General de la Policía o de la Dirección General la Guardia Civil, según el caso, que darán por recibida la información por el mismo sistema.

[42] PNR: Passenger Name Record (Registro de Nombre de Pasajeros) contiene toda la información necesaria de cada viajero para la tramitación, reserva y el control por parte de las compañías aéreas. Con ella se elabora una base de datos con información personal, tales como el nombre, apellido, número de pasaporte o documento nacional de identidad, número de teléfono, dirección; información de carácter financiero, como la forma de pago y el número de tarjeta con la que se realizó la reserva; los datos propios del viaje: fechas, itinerario, datos del billete, número de asiento, equipaje. Adicionalmente, puede contener información calificada como "suplementaria", que incluye datos sobre billetes sólo de ida, situación de *stand by* y situación de "no presentados"; y otros servicios, sobre servicios especiales solicitados. Por último, la información recopilada debe contener todo el historial de cambios de los datos de PNR DIRECTIVA 2004/82/CE del Consejo 29

de los datos obtenidos por diversas fuentes y que pueden ser cedidos a las Fuerzas de Seguridad[43], integrados en un sistema de tratamiento automatizado puede proporcionar precisa información sobre la actividad de una persona.

7. Sistemas de tratamiento y gestión de datos

En íntima relación con lo expresado en el apartado anterior, el cada vez mayor número de datos obtenido por los cuerpos policiales, obliga al tratamiento mediante sistemas integrales de información masiva.

Un ejemplo de estos sistemas es el SIGO (Sistema Integral de Gestión Operativa) de la Guardia Civil. El proyecto SIGO se complementa con los dos sistemas siguientes. El Sistema de Investigaciones, el proyecto SINVES, que es una herramienta que permitirá el seguimiento y coordinación de las investigaciones llevadas a cabo por las distintas unidades de la Guardia Civil (...) y el Sistema de Mando y Control, que permitirá la conducción y seguimiento de las distintas operaciones en las que participen unidades de la Guardia Civil que integrarán las aplicaciones de seguridad ciudadana[44].

Las líneas de trabajo futuro se encaminan a la promover la integración de sistemas entre las distintas instituciones de modo que a la hora de investigar sobre una persona concreta el sistema de investigación sea capaz de atacar la información de ficheros que usan otras instituciones, públicas o privadas, y proporcione a los investigadores, de forma rápida y automática, si se ha alojado en algún hotel, si ha

de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

43 La Agencia Española de Protección de Datos se ha pronunciado a favor de la cesión de datos a la policía Judicial en el marco de una investigación. Según la AEPD, (Informe Jurídico de la AEPD 433/200) el artículo 22.2 de la LO 15/1995 de Protección de datos de carácter personal, habilita a los miembros de las Fuerzas y Cuerpos de Seguridad para la obtención y tratamiento de los datos requeridos, lo que llevará aparejada la procedencia de la cesión instada, siempre y cuando, tal y como ha venido indicando reiteradamente la Agencia en diversos informes, se cumplan las siguientes condiciones:
– Que quede debidamente acreditado que la obtención de datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.
– Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.
– Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.
– Que en cumplimiento del artículo 22.4 de la Ley Orgánica 15/1999, los datos sean cancelados, cuando no sena necesarios para las averiguaciones que motivaron su almacenamiento.

44 Intervención del Director General de la Guardia Civil el 20 de noviembre de 2006 en el Senado. Comisiones núm. 396. http://www.senado.es/legis8/publicaciones/html/maestro/index_CS0396.html

viajado en avión, si su matrícula ha sido registrada, su datos económicos y movimientos bancarios, si ha acudido a una consulta médica, dónde está empadronado, si ha sido detectado por un sistema de videovigilancia con capacidad de análisis biométrico,... y un largo etcétera. Los límites futuros, que no técnicos, habrán de ser buscados en los mecanismos legales de control existentes y los que establezcan, que habrán de evolucionar de la forma más pareja posible a la potencial injerencia que propician estos medios sobre el derecho fundamental a la intimidad.

IV. SMARTPHONE Y LOS SERVICIOS CON VALOR AÑADIDO

Hemos hecho un somero análisis de los medios técnicos de los que, para la localización y seguimiento (y tratamiento de los datos obtenidos) se valen los investigadores de los cuerpos policiales, su potencial actual y futuro. En especial podemos resaltar por su cotidianeidad la localización mediante teléfonos móviles a través del sistema SITEL y mediante balizas, especialmente aquellas que se basan en GPS.

En este caso, lejos de sofisticados sistemas de ficción, debemos llamar la atención sobre el potencial que en el campo de la geolocalización desempeñan los teléfonos móviles de última generación. Estos terminales telefónicos, se valen del sistema UTMS que permite trasmitir los datos en banda ancha, algo que hasta ahora sólo estaba reservado a los ordenadores a través de internet. La nueva tecnología está haciendo que estos equipos portátiles se conviertan en auténticos ordenadores pero con una notable característica sobre los últimos: su alta movilidad y reducido tamaño. La versatilidad y altas prestaciones que confluyen en estos artilugios, hace que los teléfonos móviles se hayan convertido en un objeto de investigación pero también, en un instrumento —mediato— a través del que se efectúan investigaciones sobre personas y objetos.

La mayoría de usuarios de telefonía móvil de última generación, en especial los denominados *smartphones*[45], incorporan GPS al tiempo que establecen comunicación mediante redes GSM y WLAN[46] (Wi-Fi). Esto significa que un solo aparato integra varias de las tecnologías que hemos descrito y permiten que nuestro teléfono pueda ser ubicado geográficamente con un mínimo margen de error. De ahí que se estén comercializando servicios[47], que pueden ser de gran utilidad, mediante los que se ofrece la localización geográfica del terminal y por ende del que lo porta (por ejemplo el que porte nuestro hijo, el sistema antirrobo de un vehículo, etc.). Dicho de una forma coloquial, los usuarios de teléfonos de última generación portan en sus bolsillos una baliza de altas prestaciones que permite su geolocalización

45 Denominación inglesa "teléfono inteligente".

46 Sistema de comunicación inalámbrica mediante ondas. El sistema estandarizado más conocido es el IEEE 802.11. WIFI.

47 Vid. nota 21.

con una gran precisión y seguimiento de sus movimientos en un ámbito temporal extenso.

Se llaman servicios de valor añadido aquellos que elaboran información primaria para hacerla más útil a los usuarios en diferentes etapas que van desde los datos iniciales hasta la consecución de información elaborada que permite su compresión y gana en utilidad al facilitar la toma de decisiones y resolver problemas. Estamos ante el caso del tratamiento automatizado de datos primarios (datos en bruto) obtenidos mediante la integración de varios sistemas tecnológicos, en este caso, principalmente, GSM-UMTS, GPS e internet (inalámbrica WLAN-Wi-Fi) y la presentación de un resultado comprensible (información elaborada): la posición en un mapa, coordenadas geográficas, itinerarios seguidos, tiempos de permanencia en lugares concretos, etc. Si a día de hoy los cuerpos policiales, en cuanto policía judicial, pueden dirigirse a los operadores de telefonía para solicitar datos que facilitan la localización de terminales telefónicos, nada habría de impedir que también lo hagan a los proveedores de servicios de valor añadido.

Recientemente el GT-29[48] se ha pronunciado sobre los servicios con valor añadido, en concreto la geolocalización, que puede proporcionarse a través de los teléfonos de última generación (smartphones), con la conclusión[49] de que las tecnologías de geolocalización, con los datos obtenidos a través de estaciones base (BTS), GPS y mapa de puntos de acceso Wi-Fi, los dispositivos móviles pueden ser rastreados para propósitos que van desde la publicidad a la vigilancia. Considera el grupo de expertos que los patrones de movimiento obtenidos sobre el terminal proporcionan una visión "*muy íntima*" en la vida privada de sus propietarios. "Uno de los grandes riesgos es que sus propietarios no son conscientes de que transmiten sus datos de ubicación, y a quién".

Ya nos hemos referido al valor no absoluto del derecho a la intimidad por cuanto puede ser objeto de restricción. Es lógico pensar que si son legítimos los medios tradicionales de vigilancia física por parte de los agentes, no dejará de serlo por el mero hecho de que éstos se valgan de medios técnicos de apoyo. Para algunos autores auxiliarse de medios que evitan el contacto físico y aportan información objetiva supone una injerencia menor en la esfera privada[50], opinión que no podemos compartir totalmente en lo relativo al menor grado de lesividad que supone el uso de un medio incapaz de discriminar la información y que propicia el tratamiento masivo de datos personales, frente a las limitaciones que, en la captación y tratamiento, presentan los equipos humanos de vigilancia y control, además de la mayor capacidad de los últimos para discriminar datos de la intimidad que no son útiles para la concreta investigación.

El seguimiento y control mediante medios remotos, como las balizas, suponen una innegable injerencia en el derecho a la intimidad, aunque sea considerado, a priori, de menor severidad que la grabación por vídeo y audio de una persona investigada, si bien no cabe duda que el conocimiento de los movimientos de una persona incide sobre el derecho a la intimidad, sin perjuicio de que ese derecho deba ceder ante la protección de otros bienes jurídicos de relevancia constitucional.

La legitimidad del uso de balizas como medio de investigación, fue clarificada por el Tribunal Supremo en Sentencia de fecha 22 de junio de 2007, entendiendo que no hubo injerencia en ninguno de los ámbitos de intimidad protegidos, luego no se interfirió en un derecho fundamental que requiriese autorización judicial:"*... denuncian la vulneración de su derecho fundamental a un proceso debido y a la intimidad que concretan en el hecho de haber colocado una baliza de seguimiento sin autorización judicial.*

La sentencia impugnada da respuesta a la pretensión deducida como motivo de casación con una argumentación que ha de ser reproducida para la desestimación del motivo. El artificio colocado permitió a los agentes de investigación el seguimiento por mar de la embarcación respecto a la que existían fundadas sospechas de su dedicación al tráfico de drogas. La colocación de esta baliza permitió realizar el seguimiento de la embarcación, ubicarla en alta mar y para su colocación, en los exteriores del barco, no se precisó ninguna injerencia en ámbitos de intimidad constitucionalmente protegidos. Se trata, en definitiva, de un diligencia de investigación, legítima desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiriera en un derecho fundamental que requería intervención judicial".

En el mismo sentido se ha pronunciado el Tribunal Supremo con respecto a la utilización del sistema de localización que permite SITEL, en cuanto considera no afectado el derecho a la intimidad, por un lado, siempre que no se obtenga la localización con ocasión de la realización de un comunicación telefónica[51] y, por otro, siempre que la localización ofrecida sea aproximada, por zonas o con márgenes de error de cientos de metros.

- En cuanto a la no incidencia sobre una llamada telefónica (STS, 14 junio de 2006). La captación de números IMSI[52], que permiten la localización y que permiten averiguar su localización en cada momento previo cruce con las

48 ARTICLE 29 Data Protection Workin Party. Opinión 13/2001 on Geolocalitation services on smart mobile devices. http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

49 GT29. Opinión 13/2001 on Geolocalitation services on smart mobile devices., adoptada en 16 de mayo de 2011.

50 Llamas Fernández, M. y Gordillo Luque. Jm., "Medios técnicos de vigilancia", pág. 230, en la obra, Los *nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Cuadernos de Derecho Judicial. Consejo General del Poder Judicial. Madrid. 2007.

51 STS, 14 de junio de 2006.

52 IMSI: *International Mobile Subscriber Identity*-Identidad de abonado móvil mundial, es un código de identificación único para cada dispositivo de telefonía móvil, que se encuentra almacenado en la tarjeta SIM y que permite la identificación del abonado a través de las redes GSM y UMTS.

correspondientes bases de datos, no está incluida en la protección del artículo 18.3 de la Constitución Española, dado que no hay interceptación de comunicación, según jurisprudencia del TS (STS 249/2008, de 20 de mayo).

- En relación a que la afección sobre la intimidad viene dada por la precisión en la localización, el TS en sentencia 906/2008, de 19 de diciembre, "…. *Respecto de la utilización de herramientas electrónicas, sistema GPS*[53]*, que pudieran producir injerencias, no autorizadas, en la intimidad del investigado, al permitir entre otras utilidades, que fuera especialmente ubicado, el propio Tribunal de instancia, con todo acierto, se encarga de replicar este extremo afirmando que, en efecto, podría asistirle la razón al recurrente si esa localización (SITEL o Sistema de Intervención Telefónica) permitiera conocer el lugar exacto en el que el comunicante se encontraba, pero que, cuando como en este caso, esa ubicación sólo puede concretarse con una aproximación de varios cientos de metros, que es la zona cubierta por la BTS o estación repetidora que capta la señal, en modo alguno puede considerarse afectado, al menos de forma relevante, el derecho a la intimidad del sometido a la práctica de diligencia*".
- En la misma línea la Audiencia Provincial de Madrid[54] al afirmar que la localización del terminal de telefonía móvil podría significar una injerencia en el derecho a la intimidad en aquellos casos en que se pudiera determinar con exactitud el lugar exacto, edificio, vivienda, local, etc., del la persona que realiza la comunicación.
- La STS 532/2008, de 11 de julio, señala la necesariedad de acceso al domicilio para considerar infringido el derecho fundamental "*no consta que para situar el artilugio fuera necesario entrar en algún recinto que constituyera un domicilio de los previstos en los arts. 554 o 561 de la LECrm. Atendidos los documentos (…) y las declaraciones en el juicio oral de los funcionarios del SVA con números (…) respecto a la colocación exterior de la baliza en la magistral. Por otra parte, nada permite afirmar que la baliza fuera utilizada para clase alguna de injerencia en las conversaciones o mensajes de los investigados*"
- En un sentido similar se pronunció La Corte Suprema de los Estados Unidos sobre el uso de dispositivos de seguimiento, haciendo una distinción entre los espacios privados y públicos. En el caso *United Status v. Karo* [468. U.S. 707. 714 (1984)] sentenció que el dispositivo de localización afectaba a la expectativa de intimidad, dado que estaba monitorizando los movimientos

53 Cabe reseñar el error en que incurre el ponente, pues el instrumento de localización usado por la policía judicial no fue ningún dispositivo GPS sino a través de SITEL.

54 Sentencia 27/2008, de 21 de febrero (Secc. 15ª).

dentro de su domicilio[55], concluyendo la legitimidad en espacios públicos pero no en espacios privados.

En este sentido PÉREZ GIL, afirma que si no se ha entrado en el domicilio para colocar el artificio técnico que permita la localización no se puede decir que concurra la infracción al derecho a la inviolabilidad, aunque el seguimiento tenga lugar cuando el objetivo se encuentra en su propio domicilio. Sin embargo no debemos olvidar que en ocasiones el dispositivo técnico que permite el control es el teléfono del propio investigado, o bien el artilugio de seguimiento se incorpora a objetos que se hacen llegar al objetivo y es él mismo —siendo utilizado como un mero instrumento— el que lo introduce, inconscientemente, en su domicilio. De hacerse sin previa autorización judicial podríamos plantearnos si se trata de una violación de la intimidad domiciliaria en su modalidad de autoría mediata[56], al valerse de una persona cuya voluntad no entra en juego y que desconoce que está introduciendo en su esfera de intimidad un instrumento de localización y seguimiento que, en ocasiones, dada su precisión —por combinación de sistemas— permite la ubicación con una notable exactitud y que incluso existe tecnología que permite activar el micrófono de propio teléfono móvil de forma remota[57].

Nuestro Tribunal Supremo parece únicamente centrado en los aspectos formales, en cómo y dónde se obtiene, más que en el propio contenido a la hora de fijar limitaciones a la adquisición de los datos de localización. Sin embargo se hace necesario contemplar, sin duda cada vez más en el futuro, la propia información en sí misma considerada[58], así como su magnitud y potencialidad para afectar a derechos fundamentales que habrán de pasar por el filtro de la ponderación y proporcionalidad de los bienes jurídicos en juego[59].

55 PÉREZ GIL, J.: "Los datos sobre localización geográfica en la investigación penal", pág. 314, en la obra *Protección de Datos y Proceso Penal*, Ed. La Ley, Madrid, 2010.

56 Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Artículo 28. Son autores quienes realizan el hecho por sí solos, conjuntamente o por medio de otro del que se sirven como instrumento.

57 LLAMAS FERNÁNDEZ, M. Y GORDILLO LUQUE. J.M., "Medios técnicos de vigilancia", pág. 237, en la obra, "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia", Cuadernos de Derecho Judicial. Consejo General del Poder Judicial. Madrid. 2007.

58 Sin duda podemos plantear ejemplos de actividades que siendo de ámbito estrictamente privadas e íntimas —sin olvidarnos de su carácter subjetivo—, en parte, han de desarrollarse en esferas públicas, no por voluntad del afectado sino porqué no tiene otra opción. Podríamos hablar del caso de una persona que visita frecuentemente una clínica de fertilidad asistida para someterse a uno de sus tratamientos. Es posible que la persona investigada desee que su problema quede en la más estricta intimidad, cosa que habría ocurrido de no haber sido sometido a un proceso de vigilancia, que ni tan siquiera ha requerido mandamiento judicial. Los investigadores estarían obteniendo datos de la intimidad que no guardan relación alguna con hechos objeto de investigación.

59 PÉREZ GIL, J.: "Los datos sobre localización geográfica en la investigación penal", pág. 322, en la obra *Protección de Datos y Proceso Penal*. Ed. La Ley, Madrid, 2010.

Siendo conscientes de la posibilidad de que a través de los datos que de forma indiscriminada se obtienen por medios técnicos se puedan elaborar patrones de comportamiento, como es el caso de los seguimientos bien sea con SITEL o cualquier otro —y que pueden ser complementados (automáticamente) mediante los obtenidos por otros sistemas—, es difícil compartir plenamente la doctrina del Tribunal Supremo que legitima la injerencia sobre el derecho fundamental a la intimidad siempre que la localización no esté vinculada a una comunicación telefónica o suponga el conocimiento exacto de la ubicación, o se hayan invadido esferas de la intimidad domiciliaria a la hora de colocar el artificio técnico que permite el seguimiento[60].

El Tribunal está equiparando el seguimiento realizado mediante un medio técnico al seguimiento convencional. Si es cierto que el medio técnico gana en objetividad también lo es que su capacidad en la obtención indiscriminada de datos de localización y seguimiento, y de forma constante, tiene una mayor incidencia sobre la intimidad, permitiendo la elaboración de perfiles de conducta que pueden ser ajenos a la investigación concreta de un hecho delictivo. A la hora de analizar la incidencia sobre la protección de la intimidad, parece olvidarse el TS que el empleo de medios técnicos supone un avance cuantitativo y cualitativo respecto de la mera observación y percepción directa del agente, superando las capacidades humanas y obteniendo resultados que sin el uso de medios técnicos sería imposible conseguir, hasta el punto, como venimos manteniendo, de lograr perfiles de comportamiento cuyo conocimiento podrían exceden la proporcionalidad en cuanto a la invasión de un derecho fundamental.

LÓPEZ ORTEGA hace una reflexión al preguntarse por qué la jurisprudencia se muestra tan reacia a reconocer que la tutela de la intimidad se ve afectada por diligencias de investigación como las que venimos tratando. Encuentra la explicación en la resistencia, por parte de los tribunales, a reconocer que "*...junto a una dimensión territorial, la intimidad también incorpora una dimensión informativa, esta última referida al control de los datos e informaciones que son relevantes para la persona...*"[61]. Sin embargo no debemos desconocer un progresivo reconocimiento por parte de la jurisprudencia de esa dimensión informativa en los últimos años, llegando a consolidarse el derecho a la protección de datos y autodeterminación informativa como un derecho fundamental autónomo[62]. El reconocimiento supone un gran avance si consideramos que la intromisión física va cediendo paso, cada vez más, a la intromisión informativa, lo que acarrea la necesidad de trasladar a la fase procesal (en nuestro caso diligencias de investigación) la idea de la autodeterminación informativa como derecho fundamental que ha de servir de límite frente a las investigaciones discretas que se realizan con desconocimiento del vigilado, en el entendimiento de que el uso de medios técnicos, al tiempo que mejoran la discreción en la obtención de información, proporciona un control sistemático sobre la persona objeto de investigación. Es por lo que el alto potencial que presentan los nuevos medios técnicos necesitan ser dotados de una precisa regulación que establezca los límites en su uso, con fin de salvaguardar la libertad e intimidad de las personas y la validez de las investigaciones.

VI. REQUISITOS DE LEGITIMACIÓN DE LOS MEDIOS DE LOCALIZACIÓN Y SEGUIMIENTO

Nuestro ordenamiento jurídico es exiguo en la regulación de los medios técnicos de vigilancia, tanto que nuestra normativa procesal penal únicamente contiene una mínima regulación de la intervención de las comunicaciones telefónicas, déficit que ha sido y está siéndolo paliado —ante la aparición de nuevas tecnologías— por la doctrina judicial.

Nos referiremos a los presupuestos que se hacen necesarios para admitir la legitimidad del uso de medios técnicos de vigilancia, en especial aquellos que, frente a los sistemas más incisivos que permiten la captación de audio y video, sólo proporcionan la ubicación física (en un solo momento o de forma continua) del investigado —y por tanto de menor incidencia en la intimidad—, pero en el convencimiento de que los medios técnicos permiten un seguimiento tan riguroso que, puesto en contacto con otros datos mediante su procesamiento masivo y automatizado, permite conformar perfiles de comportamiento que, como ya dijimos, pueden convertir al investigado en una persona "transparente".

Para que se pueda producir la injerencia en el ámbito de protección de la intimidad, es preciso[63]:

---

60 STS 532/2008, de 11 de julio.

61 En este sentido LÓPEZ ORTEGA, J. J.:"Utilización de medios técnicos de observación y vigilancia en el proceso penal", págs, 277 y 278, en la obra "La protección Jurídica de la Intimidad", Ed. Iustel, Madrid. 2010.

62 SSTC 290/2000 y 292/2000.

63 STC 166/1999, de 27 de septiembre, en relación a la restricción de derechos fundamentales: "...sólo puede entenderse constitucionalmente legítima desde la perspectiva de este derecho fundamental si, en primer lugar, está legalmente prevista con suficiente precisión —principio de legalidad formal y material— (STC 49/1999, fundamento jurídico 4º); si, en segundo lugar, se autoriza por autoridad judicial en el marco de un proceso (STC 49/1999,) fundamento jurídico 6º.), y si, en tercer lugar, se realiza con estricta observancia del principio de proporcionalidad (STC 49/1999, fundamento jurídico 7º.); es decir, si la medida se autoriza por ser necesaria para alcanzar un fin constitucionalmente legítimo, como —entre otros—, para la defensa del orden y prevención de delitos calificables de infracciones punibles graves, y es idónea e imprescindible para la investigación de los mismos (ATC 344/1990, SSTC 85/1994, fundamento jurídico 3º, 181/1995, fundamento jurídico 5º., 49/1996, fundamento jurídico 3º., 54/1996, fundamentos jurídicos 7º. y 8º., 123/1997, fundamento jurídico 4º.; SSTEDH casos Huvig y Kruslin, y Valenzuela)".

- Que exista un fin de interés público con relevancia constitucional que justifique la ingerencia[64].
- Que la intromisión en la esfera de la intimidad tenga previsión legal suficiente.
- Que la injerencia sea autorizada por autoridad judicial si es grave.
- Que en se respete el principio de proporcionalidad[65] en su adopción y ejecución, en sus vertientes de idoneidad, necesariedad y proporcionalidad en sentido estricto.
- Excepcionales injerencias que no requieren autorización judicial previa[66].
- Información al objetivo de la vigilancia efectuada sobre el mismo a su finalización[67].

1. *Existencia de fin legítimo*

La intromisión e injerencia en el ámbito de un derecho fundamental no puede tener otro fin que la salvaguarde derechos, bienes o valores de relevancia constitucional. En ese marco se desenvuelve el esclarecimiento de los delitos y descubrimiento de sus responsables. Es por ello que la intervención requiera la preexistencia de un supuesto delito, lo que impide que las intromisiones en el ámbito de los derechos fundamentales se realicen con mero carácter preventivo o prospectivo.

64 STC 14/2003 de 28 de enero "Al respecto debe advertirse que reviste relevancia e interés público la información sobre los resultados positivos o negativos que alcanzan en sus investigaciones las fuerzas y cuerpos de seguridad, especialmente si los delitos cometidos entrañan una cierta gravedad o han causado un impacto considerable en la opinión pública, extendiéndose aquella relevancia o interés a cuantos datos o hechos novedosos puedan ir descubriéndose por las más diversas vías, en el curso de las investigaciones dirigidas al esclarecimiento de su autoría, causas y circunstancias del hecho delictivo (SSTC 219/1992, de 3 de diciembre, FJ 4; 232/1993, de 12 de julio, FJ 4; 52/2002, de 25 de febrero, FJ 8; 121/2002, de 20 de mayo, FJ 4; 185/2002, de 14 de octubre, FJ 4). Pues bien, en el presente caso no puede estimarse que la intromisión que ha padecido el recurrente en amparo en su derecho a la propia imagen se encuentre justificada por los distintos bienes constitucionales e intereses públicos aducidos…"

65 Desde la STC 37/1989, de 15 de febrero, se conoce con el nombre de regla de la proporcionalidad de los sacrificios el conjunto de requisitos (especialmente de motivación) necesarios para llevar a cabo la limitación de un derecho fundamental.

66 STC 37/1998.

67 STS 89/2006 "… si la intimidad e, entre otras facetas, una reserva de conocimiento de un ámbito personal, que por eso denominamos privado y que administra su titular, tal administración y tal reserva se devalúan si el titular del ámbito de intimidad desconoce las dimensiones del mismo porque desconoce la efectiva intromisión ajena. Tal devaluación es correlativa a la de la libertad, a la de la "calidad mínima de la vida humana" (STC 231/1988, de 2 de diciembre, FJ 3º), que posibilita no sólo un ámbito de intimidad, sino el conocimiento cabal del mismo".

Por tanto es preciso, antes de adoptar la medida invasiva, la existencia de un ilícito penal de suficiente gravedad y que la medida a adoptar esté encaminada al esclarecimiento de ese concreto delito. En palabras del Tribunal Constitucional se requiere que la sospecha de comisión del delito y responsabilidad en el mismo por parte del investigado sea de "cierta entidad" y que permita pueda ampararse la existencia de una sospecha fundada en datos objetivos, siendo relevante que esos datos objetivos han de ser accesibles a terceros[68]. No obstante, se ha pronunciado el Tribunal Constitucional en un supuesto[69], legitimando la restricción del derecho a la intimidad a favor del carácter preventivo de la seguridad pública cuando esta invasión se realiza sobre actividades que transcurren en espacios públicos, dado que se trata una injerencia de una intensidad más leve, si bien, es preciso detallar que la intervención de la que se ocupa del TC se refiere a la filmación de un hecho concreto, referido a la actuación de un piquete informativo en el desempeño de sus funciones informativas y, en consecuencia, limitado en el espacio y el tiempo.

En suma, a la vista de estos datos, puede concluirse que en el presente caso concurría la existencia de un bien constitucionalmente legítimo como es la protección de los derechos y libertades de los ciudadanos y la preservación de la seguridad ciudadana que, en principio, podía justificar la adopción de una medida de control preventivo *(…) Al ser pública la actuación del piquete, la sentencia descarta que la mera filmación coarte los derechos a la intimidad personal y a la propia imagen y de reunión y manifestación, estando amparada por el art. 103.1 CE(…)* STC 37/1998, de 17 de febrero.

Cabe llamar la atención sobre lo que GONZÁLEZ LÓPEZ[70] ha denominado *"investigación pro activa"* como nueva metodología de investigación que afronta el modo de abordar la delincuencia organizada. Hasta ahora las investigaciones siempre ha sido una reacción a la comisión de un delito. Sin embargo, la delincuencia organizada y de base estable provoca que no sólo se reaccione ante la comisión de un delito concreto, sino que se hace necesario investigar el "entorno" delictivo desde una perspectiva no sólo reactiva sino pro activa, con el fin de investigar delitos cometidos y los que se están cometiendo pero que aún no son conocidos, sin olvidar que la mera pertenencia a una banda organizada constituye por sí una actividad delictiva que puede convertirse en el indicio que permita la injerencia.

68 STC 184/2003. "… pero las sospechas precisan, para que puedan entenderse fundadas, hallarse apoyadas en datos objetivos, que han de serlo en un doble sentido. En primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control. Y, en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o se va a cometer el delito sin que puedan consistir en valoraciones acerca de la persona".

69 STC 37/1998 de 17 de febrero.

70 GONZÁLEZ LÓPEZ, J.J.: *Los datos de tráfico de las comunicaciones electrónicas en el proceso penal*, Ed. La Ley. Madrid, 2007, pág. 77

Siguiendo la argumentación del TC difícilmente podríamos concluir la legitimidad de la localización y seguimiento de una persona por medios tecnológicos sin previa existencia de una base indiciaria de comisión de delito o *in extremis* de su pertenencia a una organización delictiva, dado que los medios tecnológicos no pueden distinguir entre la actividad que se desempeña en lugares públicos o aquellos que pertenecen a la esfera más íntima, pudiendo afectarse ámbitos de la intimidad que ninguna relación guarden con actos ilícitos y que, a diferencia de la vigilancia directa, el sistema técnico no sabrá discriminar.

2. *Previsión legal suficiente*

Cualquier restricción o intromisión en el ámbito de un derecho fundamental ha de estar prevista en una norma con rango de ley que describa el alcance y características de la injerencia o limitación del derecho. No basta la existencia de la norma sino que, además, debe cumplir ciertos requisitos de calidad, como afirma el TEDH, en "*términos suficientemente claros para indicar a todos en qué circunstancias y bajo qué condiciones habilita a los poderes públicos para adoptar medidas secretas*"[71]. La necesidad de previsión legal específica para las medidas que supongan una injerencia en los derechos a la intimidad y a la integridad física está establecida en el art. 8 CEDH[72], en la medida en que la jurisprudencia del TEDH incluye todos los derechos dentro del más genérico derecho del respeto a la vida privada y familiar (STEDH "Costello-Roberts/Reino Unido" de 25-3-1993 entre otras).

Sin embargo, pese a la contundencia con que se pronuncia el TEDH, nuestro Tribunal Constitucional, con ocasión de las escuchas telefónicas, y tras reconocer la insuficiencia de la ley[73] que regula las intervenciones, estableció la validez de las escuchas realizadas con base en la jurisprudencia siempre que las intervenciones hubiesen sido acordadas por autoridad judicial.

> *(...) si, pese a la inexistencia de una ley que satisficiera las genéricas exigencias constitucionales de seguridad jurídica, los órganos judiciales, a los que el art. 18.3 de la Constitución se remite, hubieran actuado en el marco de la investigación de una infracción grave, para la que de modo patente hubiera sido necesaria, adecuada y proporcionada la intervención telefónica y la hubiesen acordado respecto de personas presuntamente implicadas en el mismo, respetando, además, las exigencias constitucionales dimanantes del principio de proporcionalidad, no cabría entender que el Juez hubiese vulnerado, por la sola ausencia de dicha ley, el derecho al secreto de las comunicaciones telefónicas* (STC 49/1999).

En el caso que nos ocupa, la injerencia en el ámbito de la intimidad mediante medios técnicos que permiten conocer la ubicación física y el seguimiento, la regulación legal no es insuficiente sino inexistente y ante la duda de la posibilidad de "convalidación" mediante resolución judicial, como vimos, la STS de fecha 22 de junio de 2007, entendió que no era necesaria autorización judicial pues no hubo injerencia en ninguno de los ámbitos de intimidad protegidos cuando se colocó una baliza de seguimiento en una embarcación, *"sin que en su colocación se interfiriera en un derecho fundamental que requería intervención judicial"*, doctrina difícil de extrapolar, a nuestro juicio, a casos en los que el seguimiento se hace a través de un teléfono móvil de última generación, que es portado de forma casi constante por una persona (y no por un medio de transporte) y actúa indiscriminadamente incluso en el interior de espacios protegidos por la inviolabilidad domiciliaria. Lo dicho, ha de ser agravado con que, la localización mantenida en el tiempo —seguimiento— ofrece no solo datos de localización sino que permite elaborar perfiles de comportamiento y que nos pueden llevar a conocer datos especialmente protegidos como aquellos relativos a la salud, condición sexual, etc., que no guarden relación con el hecho delictivo que se estuviese investigando. En conclusión nos encontraríamos con que el TC admite que la ausencia de ley puede ser suplida por la intervención judicial previa y el TS admita (también lo hace el TC —como veremos en el siguiente epígrafe—) la no necesidad de resolución judicial en el caso de injerencias leves.

En el ánimo de encontrar la ley que pudiera legitimar las diligencias de investigación podríamos pensar, en el caso de localizaciones y seguimientos a través de SITEL, que la injerencia en el derecho fundamental a la intimidad puede ser una extensión de la posibilidad de intervenir una comunicación, entendiendo que se hace valiéndose de mandamiento judicial. Sin embargo, ninguna interpretación extensiva habría de convertir en legítima la restricción del derecho que no esté expresamente previsto en una ley, pues es precisa una norma que regule los casos concretos y formas en que puede realizarse la intromisión. Si el artículo 579 de la LECrim es deficitario en la regulación de las intervenciones telefónicas, más lo es aquella norma que sencillamente no existe, como ocurre con los seguimientos mediante medios tecnológicos.

---

71 STEDH caso Malone contra Reino Unido. 1984.

72 Artículo 8.2 del Convenio para la protección de los derechos y de las libertades fundamentales hecho en Roma el 4 de noviembre de 1950. "No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para 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 las libertades de los demás.

73 STC 49/1999 "La intervención telefónica, encuentra su deficitaria regulación en el artículo 579 de la Ley de Enjuiciamiento Criminal, según su redacción de redacción mediante Ley Orgánica 4/1988, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal".

Tampoco, en ausencia de ley específica, deberíamos acudir a las atribuciones genéricas como la del artículo 282[74] de la LECrim cuando establece que la policía judicial practicará las diligencias necesarias para comprobar los delitos y descubrir a los delincuentes, pues es clara la doctrina del TEDH. Lamentablemente, los esfuerzos de los tribunales por suplir las carencias de una regulación deficitaria en unos casos e inexistente en otros, sin dudar de la buena voluntad de los juzgadores, al final nos conducen a una inevitable intromisión del Poder Judicial en las competencias del Legislativo ante la falta de capacidad del último para abordar y regular las nuevas situaciones que generan los medios tecnológicos en el ámbito de la investigación procesal y la protección de los derechos fundamentales.

Artículo 33.2 de la Ley 32/2003 General de Telecomunicaciones, en sintonía con cuanto venimos manteniendo y en concordancia con la doctrina del TEDH, establece que "*Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de Ley Orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes*", no habiendo omitido la necesidad de que dicha previsión —al afectar a un derecho fundamental— deba ser regulado mediante Ley Orgánica[75], regulación del empleo de medios técnicos de localización y seguimientos hoy inexistente, pues si forzar el artículo 579 pudiera ampararnos en algunos casos, quedamos huérfanos de ley cuando se utilicen medios en los que no intervengan los operadores telefónicos.

3. *Autorización judicial previa*

Con respecto a la injerencia en el derecho a la intimidad (art. 18.1 CE) no existe la reserva absoluta de previa resolución judicial a diferencia de otras injerencias que, ineludiblemente, han de ir precedidas del mandato judicial, como es la restricción del secreto a las comunicaciones. Así lo ha aclarado el Tribunal Constitucional en Sentencia 233/2005.

La STC 70/2002 sienta la posibilidad de injerencias de carácter leve por parte de la policía judicial sin autorización del juez, con carácter excepcional, si existen razones de urgencia y se respeta el principio de proporcionalidad en la actuación si sus fines son el aseguramiento de la prueba, sin olvidar, como ya dijimos en el

74 Art. 282. La Policía judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la Autoridad Judicial.

75 Art. 81 Constitución Española.

apartado anterior, siempre que exista una habilitación legal que legitime la actuación[76]. BUENO GALLARDO[77] explica el análisis de la jurisprudencia nos lleva a afirmar que la intervención judicial sólo es obligatoria cuando las injerencias sobre el derecho con de la máxima gravedad.

Respecto del seguimiento y control de localización de una persona, que se suele prolongar en el tiempo, si bien pudiera justificarse su inicio sin autorización judicial, en base a razones de urgencia, difícilmente podría entenderse que no se someta a revisión y autorización judicial, en su caso, tan pronto como sea posible, el mantenimiento de una medida prolongada en el tiempo que, sin duda, afecta a la intimidad.

El problema lo encontramos a la hora de considerar el grado de incidencia o lesividad en el derecho. Suele ser pacífica la consideración de que los datos captados en lugares públicos tienen una escasa incidencia sobre la intimidad, ya que en los espacios públicos cualquiera es consciente de estar sometido a la observación de terceros. LÓPEZ ORTEGA[78] distingue la localización y seguimiento que se hace mediante el teléfono que porta el objetivo y la que se hace colocando artilugios de seguimiento en objetos como los medios de transporte. Coincidimos en que es distinto el grado de incidencia que se produce cuando el instrumento de localización (como las balizas) es portado por la persona que cuando es colocado en un medio de transporte. Respecto de la injerencia que se produce con un instrumento que porta la propia persona y que permite la localización constante y permanente a lo largo del tiempo y que incluso se extiende a esferas de la intimidad domiciliaria, no habría de caber duda sobre su particular lesividad, toda vez que el seguimiento constante no sólo permite obtener un dato concreto en relación a una actividad potencialmente delictiva, sino que permite trazar un perfil de comportamiento que se extiende a ámbitos de la más estricta intimidad.

Hasta ahora, el TS, en sus pronunciamientos sobre el sistema SITEL, ha afirmado que no existe injerencia en la intimidad, por la falta de precisión del sistema, al ofrecer los datos de localización con un margen de varios cientos de metros[79]. La opinión del TS para el caso concreto, no puede generalizarse por simplista, primero al obviar el potencial tecnológico y la precisión que supone la combinación de varios medios técnicos de localización y, en segundo lugar, al ignorarse el potencial de información que proporciona la localización permanente, pues la incidencia sobre el derecho a la intimidad no se produce solo al conocer la exactitud de la localización sino también, y más, por la prolongación de la medida en el tiempo.

76 STC 56/2003.

77 BUENO GALLARDO, E: *La configuración constitucional del derecho a la intimidad*, Ed. Centro de Estudios Constitucionales, Madrid, 2009. Pág. 794.

78 LÓPEZ ORTEGA, J. J:. "Utilización de medios técnicos de observación y vigilancia en el proceso penal", págs, 310 y 311, en la obra *La protección Jurídica de la Intimidad*, Ed. Iustel, Madrid. 2010.

79 TS en sentencia 906/2008, de 19 de diciembre.

A modo de ejemplo, saber que una persona está en una cafetería en un día y a una hora concreta, en principio no revela nada extraordinario, pero si sabemos que está en un bar mañana, tarde y noche, podemos llegar a otras conclusiones —al margen de una investigación concreta— como que tiene problemas de alcoholismo.

Venimos considerando la gravedad de la incidencia de la localización a través de sistema de telefonía móvil (o sistema análogo) que porta el afectado y que, en consecuencia necesita de autorización judicial cuyo contenido es preciso concretar.

Establecido como uno de los requisitos habilitadores la previa existencia de un delito, es necesario que la resolución precise cuáles son los indicios delictivos que provocan la diligencia de investigación que se concreta en el relato del hecho y vinculación a la persona supuestamente responsable. La indeterminación del alcance subjetivo y objetivo de la investigación deslegitima la resolución habilitante[80].

Debe expresar el criterio de idoneidad y necesidad de la injerencia, como medio útil al fin perseguido así como la imposibilidad de alcanzar el mismo fin mediante otro medio menos invasivo.

Descritos los hechos, indicios y vinculación subjetiva, así como expuesta la idoneidad y la imprescindibilidad de la injerencia, ponderados los bienes jurídicos en conflicto, se han de expresar las condiciones materiales específicas de ejecución de la diligencia de investigación, condiciones que, como hemos criticado, carecen de regulación en nuestro marco legal.

Frente a quienes mantienen la posibilidad de recabar datos de localización[81] sin previa autorización judicial, al amparo de la que entendemos cláusula genérica del artículo 22.2[82] de la Ley Orgánica de protección de datos de carácter personal (LOPD), que permite el acopio de datos con fines policiales sin consentimiento del interesado en este caso procedentes de un tercero —operador de telefonía—, no pueden desconocer la necesidad de interpretar dicha cláusula en concurso con los artículos 11 de la LOPD (que prevé la comunicación de datos sin consentimiento si así lo autoriza una ley; y los dirigidos a Autoridad Judicial o Ministerio Fiscal) y de Ley 25/2007, de conservación de datos (LCD) relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuyo artículo primero establece la necesidad de orden judicial para la cesión de datos

> *"Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales"*, en el mismo sentido que exige autorización judicial el Reglamento de la Ley General de Telecomunicaciones.

4. *Proporcionalidad de la medida*

La legitimidad de la diligencia de investigación que supone una ingerencia en la esfera de la intimidad demanda su proporcionalidad en términos de idoneidad, necesariedad y proporcionalidad en sentido estricto.

Ha de ser idónea para conseguir los fines que se persiguen. Difícil legitimación tendría someter a una persona a la vigilancia de su localización si lo que se pretende es tener conocimiento de sus movimientos bancarios.

Ha de ser imprescindible, por cuanto la información que se pretenda no pueda ser obtenida por un medio menos gravoso. Por ello debe entenderse el carácter subsidiario de las medidas que lesionan derechos fundamentales.

En cuanto a la proporcionalidad, en sentido estricto, ha de estar justificado el sacrificio del derecho, es decir, que el derecho a la intimidad deba ceder ante otro, de relevancia constitucional, y de mayor importancia para el interés general. Es el criterio cuya aplicación presenta mayores dificultades, pues obliga a la ponderación de los fines que persigue la injerencia con la lesión al derecho fundamental. La proporcionalidad exige que la medida esté destinada a la investigación de un delito grave. Para ello el Tribunal Constitucional considera que no sólo ha de tenerse en cuenta la pena que corresponde al delito sino también otros factores como la relevancia social de la conducta. Con ese criterio, el TC considera que forman parte de estos delitos graves aquellos cometidos por funcionarios públicos, dada la relevancia estructural para el funcionamiento del Estado y su trascendencia social, por su capacidad para socavar la confianza de los ciudadanos en aquél y sus instituciones[83]. El derecho a la intimidad, al igual que otros fundamentales, como señala el TC no es un derecho absoluto, que podrán ceder una vez sometidos al juicio de ponderación entre los bienes jurídicos que entren en conflicto.

Entendemos entonces que en el *iter* de esclarecer un delito y descubrir a sus responsables, antes de abordar una medida que suponga injerencia en el derecho

---

80 STC 54/1996.

81 Llamas Fernández, M. Y Gordillo Luque, JM.: "Medios técnicos de vigilancia", pág. 233, en la obra, *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Cuadernos de Derecho Judicial. Consejo General del Poder Judicial, Madrid, 2007.

82 Art. 22.2 de la Ley Orgánica de Protección de Datos de Carácter Personal. "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas estén limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad".

83 STC 184/2003.

a la intimidad, es obligada la ponderación de los intereses que se oponen y determinando en cada caso concreto cuál es el interés que debe prevalecer. Salvo aquellos casos que por su levedad pudieran corresponder a la autonomía de la policía judicial, el juicio de ponderación debe ser abordado por el juez, como garantía de efectividad del derecho a la intimidad, pues nunca se podría descartar la existencia de un bien tan relevante que permita restringir el derecho, incluso en sus aspectos esenciales[84].

Dentro de la proporcionalidad debemos aludir a la temporalidad de la medida, pues una injerencia en principio proporcional puede dejar de serlo si se prolonga indefinidamente o de forma injustificada[85].

La proporcionalidad no sólo exige ser tenida en cuenta a la hora de acordar la autorización de injerencia sino que obliga a mantenerla durante la ejecución, por cuanto exigirá un estricto control judicial sobre las condiciones en la que se efectúa la concreta diligencia de investigación.

5. Excepcionales injerencias sin necesidad de autorización judicial previa

A lo largo del texto nos hemos referido a injerencias que por su incidencia leve no requieren de resolución judicial previa que habilite la investigación. En la materia que nos ocupa una localización o seguimiento, cuando los instrumentos técnicos de seguimiento son colocados, por ejemplo, en los medios de transporte de los que se vale el investigado. El TS[86] considera que no es necesaria la autorización judicial cuando el seguimiento y localización se realiza mediante una baliza colocada sin necesidad de entrar en recinto con la consideración de domicilio.

Sin volver a entrar en la discusión sobre la levedad de la injerencia, que hemos cuestionado, por su posibilidad de contribuir en muchos casos a la generación de perfiles de comportamiento, es necesario reflejar que la actuación debe participar de todos los condicionantes hasta ahora expuestos. Ha de producirse en virtud de una habilitación legal suficiente y respetando el principio de proporcionalidad puesto que, aún a posteriori, la legitimidad de la actuación se encuentra sometida al control jurisdiccional que verificará la existencia de indicios objetivos, la idoneidad de la medida y su necesariedad.

84 López Ortega, J. J.: "Utilización de medios técnicos de observación y vigilancia en el proceso penal", en la obra *La protección Jurídica de la Intimidad*, Ed. Iustel, Madrid. 2010. Pág. 325.

85 El ejemplo más próximo lo encontramos en la regulación del artículo 579 de la LECrim respecto de las intervenciones telefónicas, para las que fija un plazo máximo de tres meses, sin perjuicio de posteriores prórrogas.

86 SSTS 562/2007 y 523/2008.

VII. INEXISTENCIA DE REGULACIÓN LEGAL. ¿CONSECUENCIAS?

Una muestra de lo deficitario de la normativa española en materia de prueba es que nuestra Ley de Enjuiciamiento Criminal sólo regula siete medios probatorios, encaminados a la comprobación del delito y averiguación del delincuente responsable. No queda más remedio, ante la ausencia de principios inspiradores, acudir a la interpretación analógica y a la jurisprudencia, sin olvidar de la dificultad que esto supone al movernos en el campo del derecho procesal, al servicio del derecho penal.

La falta de norma legal que regule la medida que con fin de obtener una prueba da lugar a la injerencia en el derecho fundamental, podría convertir el material probatorio obtenido en prueba ilícita[87] con las consecuencias deducibles del artículo 287 de la Ley de Enjuiciamiento Civil, de aplicación supletoria al no existir regulación igual en el orden penal, en relación con el artículo 11.1 de la Ley Orgánica del Poder Judicial[88] y 6.3 del Código Civil, permite concluir la nulidad de los actos procesales contrarios a los derechos fundamentales (que su injerencia esté regulada por ley). Además de la imposibilidad de valoración del material declarado ilícito, puede afectarse a las pruebas derivadas de aquel. No obstante, cabe añadir que elemento esencial para considerar ilícito el medio de prueba es que produzca una efectiva indefensión en la parte a quien perjudique la misma.

El déficit normativo en cuanto a los medios de investigación alcanza la cima al acercarnos al material probatorio que se obtiene a través de medios técnicos, de modo que se hace preciso, revisar caso por caso y medio por medio, la aplicación analógica con la regulación legal más semejante así como la jurisprudencia de los tribunales, si bien pesa sobre este actuación compensatoria la doctrina del TEDH que exige la existencia de Ley para que la prueba pueda obtenerse cuando implica la injerencia en un derecho fundamental.

VIII. CONCLUSIONES

La evolución de los medios tecnológicos, que no son desconocidos por los delincuentes, especialmente los que "trabajan" de forma organizada, hace que la Policía Judicial no pueda despreciar los recursos que ofrece la tecnología para contrarrestar el cada vez mayor potencial delictivo de las organizaciones crimina-

87 Urbano Castrillo, e.: "La investigación tecnológica del delito", pág. 55 y 56, en *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Cuadernos de Derecho Judicial. Consejo General del Poder Judicial, Madrid, 2007.

88 Ley Orgánica 6/1985 del Poder Judicial. Artículo 11.1. "En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales".

les. Es preciso tomar conciencia de que estas "armas" al servicio de los cuerpos policiales, en definitiva del poder público (y político), tienen un doble filo por cuanto por un lado se prestan útiles en la lucha contra el crimen pero por otro, su uso, potencia una injerencia en el derecho fundamental a la intimidad que debe ser controlado como exigencia de un estado de seguridad y libertad en el marco del estado de derecho.

Es cierto que el marco constitucional no permite construir un derecho a la intimidad de carácter absoluto, por cuanto la posibilidad de restricción debe quedar al juicio de ponderación de los intereses en conflicto. Siendo de ese modo, la injerencia en el derecho fundamental a la intimidad debemos considerarla un "sacrificio necesario" que se produce en el logro de pruebas que tienen por destino la futura formación de la convicción judicial que tiene lugar en el marco de un proceso basado en el reconocimiento de la igualdad de armas entre partes, y que no puede entenderse sino desde el prisma de la tutela judicial efectiva y la garantía de los derechos fundamentales. Es por lo que la intromisión en el ámbito de un derecho fundamental requiere cumplir con los criterios de ley previa, fin de relevancia constitucional, autorización judicial previa (salvo injerencias leves) y el respeto al principio de proporcionalidad.

Captar información relativa a una persona, cuando se hace de forma subrepticia, con independencia de la intensidad con que se haga, implica una injerencia en el derecho fundamental a la intimidad, pues supone para el afectado la pérdida de control sobre qué datos relativos a su persona son conocidos —y tratados— por terceros, una injerencia en el derecho a la autodeterminación informativa.

Desafortunadamente nuestro ordenamiento jurídico es deficitario en la regulación del uso de medios técnicos aplicados a la investigación procesal en cuanto a la geolocalización y seguimiento de personas. La participación de la doctrina judicial, en respeto a la separación de poderes, no debería ser tan intensa como lo es a día de hoy, hasta el punto que llega a suplir la inexistencia de ley. Del mismo modo que habría de ser considerada odiosa la interpretación extensiva de cláusulas generales cuando se persigue el objetivo de limitar derechos fundamentales en el marco de un proceso penal.

El déficit normativo que rodea la injerencia en el derecho a la intimidad mediante instrumentos tecnológicos concede al principio de proporcionalidad un carácter esencial a la hora de legitimar la injerencia en el derecho fundamental a la intimidad, pues la medida que pretenda adoptarse habrá de superar el juicio de necesidad e idoneidad a los efectos de obtener el material probatorio que se persigue, así como de ponderación respecto a la gravedad de los hechos y objetividad de los elementos que los atribuyen a una persona concreta. Se hace precisa una norma con rango de Ley con una concreta regulación garantista del contenido esencial del derecho y de carácter restrictivo en cuanto a las condiciones para materializar la injerencia. De otro modo se corre el riesgo, ante el juicio de ponderación, de restringir el derecho a la intimidad en cada caso en el que aparezca el conflicto, convirtiendo el derecho a la intimidad y a la autodeterminación informativa en una mera apariencia.

La ubicación de personas a través de sistemas como SITEL, que permiten geolocalizar un concreto terminal telefónico y, en consecuencia, a su portador, debiera considerarse una injerencia de la máxima gravedad ya que, por más que el Tribunal Supremo diga que no se lesiona el derecho a la intimidad por cuanto la localización que ofrece el sistema goza de un notable margen de error, es innegable que no puede valorarse únicamente la localización puntual en un momento concreto, sino que los sistemas de geolocalización —hoy llamados servicios de valor añadido— que se valen de la combinación de varias tecnologías permiten la ubicación y el seguimiento durante largos periodos de tiempo, lo que implica, no sólo ubicar con cierta precisión, sino generar perfiles de movimiento y comportamiento.

En este trabajo no nos hemos querido referir únicamente a SITEL sino que con una vocación más extensa hemos tratado los sistemas de geolocalización y hemos podido ver que las nuevas tecnologías permiten situar a una persona con un margen de error de muy pocos metros. Es por ello que la opinión del TS en cuanto a que no se incide en el derecho fundamental dado el alto margen de error en la localización únicamente podemos aceptarla con respecto al caso concreto sobre el que se pronuncia pero no como opinión generalizada de que la localización no incide en el derecho a la intimidad, al contrario, el TS se vale del margen de error para su afirmación, luego, a *contrario sensu*, acreditada la precisión de un sistema de geolocalización lo estará siendo también su incidencia —severa— en el derecho a la intimidad.

Como últimas líneas debemos alertar de la necesidad de una regulación legal, que incorpore los principios hasta ahora desarrollados por la jurisprudencia y aborde, con vocación de futuro, los potenciales de los nuevos medios técnicos al servicio de la investigación, bajo riesgo, de no hacerlo, del constante cuestionamiento de las actuaciones policiales, pérdida del trabajo operativo y pérdida de eficacia de los cuerpos policiales, así como potenciales e indeseables responsabilidades para los agentes de la policía judicial a causa de actuaciones derivadas de una confusa, deficiente y, en la mayoría de los caos, inexistente regulación.

IX. BIBLIOGRAFÍA

Asencio Mellado.: *Prueba prohibida y prueba preconstituida,* Ed. Trivium, Madrid 1989.

Avilés García, J.: *Algunas consideraciones jurisprudenciales acerca de los derechos a la intimidad y a la propia imagen*, Ed. La Ley, nº 2.284, año X, Madrid.

Bueno Gallardo, E.: *La configuración constitucional del derecho a la intimidad,* Ed. Centro de Estudios Constitucionales, Madrid, 2009.

Cabezuelo Arenas, A.L.: *Derecho a la intimidad,* Ed. Tirant lo Blanch, Valencia, 1998.
Desantes Guanter, J.M. Soria, C.: *Los límites de la información,* Ed. Asociación de la Prensa de Madrid, Madrid, 1991.
Etxebarría Guridi, J.F.: *La previsión legal de las diligencias de investigación restrictivas de derechos fundamentales (A propósito de la STC 49/1999, de 5 de abril)* Ed. La Ley, Madrid, 1999.
González López, J.J.: *Los datos de tráfico de las comunicaciones electrónicas en el proceso penal,* Ed. La Ley, Madrid, 2007.
Grimalt Servera, P.: *El derecho a controlar los datos personales,* Ed. Universidad Pontificia de Comillas, Madrid, 1997.
López Ortega, J. J.:"Utilización de medios técnicos de observación y vigilancia en el proceso penal", en la obra *La protección Jurídica de la Intimidad,* Ed. Iustel, Madrid, 2010.
Llamas Fernández, M. y Gordillo Luque, J.M.:"Medios Técnicos de Vigilancia" en la obra *Los nuevos medios de investigación en el proceso penal. Especial referencia a la Tecnovigilancia,* Ed. Cuardernos de Derecho Judicial, Madrid, 2007.
Lucas Murillo De La Cueva, P.: *El derecho a la autodeterminación informativa y la protección de datos personales,* Ed. Azpilcueta Cuadernos de Derecho 20 Donostia-San Sebastián, 2008.
Madrid Conesa, F.: *Derecho a la intimidad, informática y Estado de Derecho,* Ed. Universidad de Valencia, 1984.
Pérez Gil, J.: "Los datos sobre localización geográfica en la investigación penal", en Vv.aa *Protección de Datos y Proceso Penal,* Ed. La Ley, Madrid, 2010.
Rebollo Delgado, L.: *Derechos fundamentales y protección de datos,* Ed. Dykinson, Madrid, 2004.
Rebollo Delgaco, L.: *Vida privada y protección de datos en la Unión Europea,* Ed. Dykinson, 2008.
Ruiz Miguel, C.: *La configuración constitucional del derecho a la intimidad,* Ed. Tecnos, Madrid, 1995.
Urbano Castrillo, E.: "La investigación tecnológica del delito", en *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia,* Cuadernos de Derecho Judicial, Ed. Consejo General del Poder Judicial, Madrid, 2007.

Fuentes Internet:

III Congreso Virtual Intervisual sobre la autonomía personal de personas con ceguera o deficiencia visual. Octubre 2005.
http://juntadeandalucia.es/averroes/caidv/interdvisual/iiicv/gps_ay_orientacion_pc.pdf
Sistemas de Posicionamiento Global
http://es.wikipedia.org/wiki/Sistema_de_posicionamiento_global
Geoposicionamiento GSM independiente de la red móvil.
Criptolab. Facultad de Informática de la Universidad Politécnica de Madrid
http://www.kriptopolis.org/geoposicionamiento-gsm-1
Informes Gabinete Jurídico Agencia Española de Protección de Datos
http//:www.aepd.es
Opinión 13/2011 on Geolocation services on smart mobile devices
http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm
Article 29, Data Protection Workin Party. Opinión 13/2001 on Geolocalitation services on smart mobile devices.

Fecha de recepción: 05/07/2012
Fecha de aceptación: 1/09/2012