Facultad de Derecho
Universidad de La Laguna

Máster en Abogacía
Facultad de Derecho Universidad de La Laguna
Ilustre Colegio Abogados SC Tenerife
Curso 2019/2020
Convocatoria: septiembre

La regulación legal de la utilización de dispositivos técnicos de seguimiento y localización: especial referencia a su utilización en la pandemia COVID-19

The legal regulation of the use of technical devices for monitoring and location: special reference to its use in the COVID-19 pandemic.

Realizado por la alumna Miriam Expósito González

Tutorizado por la Profesora Juana Pilar Rodriguez Perez

Departamento: Derecho Público y Privado Especial y Derecho de la Empresa

Área de conocimiento: Derecho Procesal

C/ Padre Herrera s/n
38207 La Laguna
Santa Cruz de Tenerife, España

RESUMEN

El presente trabajo se centra en el estudio de la medida de investigación introducida en la LO 13/2015, de 5 de octubre. Concretamente la desarrollada en el capitulo VII, que introdujo los art. 588 quinquies b) y c), que lleva por titulo "la utilización de dispositivos técnicos de captación de la imagen, seguimiento y localización". Nosotros estudiaremos la medida de investigación de seguimiento y localización así como su afectación en la actual pandemia Covid-19, a través de las aplicaciones de seguimiento creadas para el control de la misma.

ABSTRACT

The present article focuses on the study of the new research measure introduced in LO 13/2015, of 5 October. Specifically the one developed in Chapter VII, which introduced the new art. 588 quinquies b) and c), whose title is as follows "the use of technical devices for image capture tracking and tracing". Throughout the work, we will study the tracking and location research measure as well as its impact on the current Covid-19 pandemic, through the monitoring applications created to control it.

Índice

Pág.

1. Introducción 4

2. Fundamento de la reforma de la Ley de Enjuiciamiento Criminal respecto a la investigación tecnológica 6

3. Disposiciones comunes a las medidas de investigación tecnológica 11

3.1 Principios rectores 11

3.2 Procedimiento para la solicitud y autorización judicial de la medida de investigación tecnológica 13

3.3 Duración de la medida 15

3.4 Control judicial de la medida de investigación tecnológica 16

3.5 Deber de colaboración 16

3.6 Cese de la medida y destrucción de los registros obtenidos 17

4. Utilización de dispositivos técnicos de seguimiento y localización 19

4.1 Clases de dispositivos técnicos de seguimiento y localización 20

4.2 Posibilidad de afectar a los Derechos Fundamentales por la utilización de dispositivos técnicos de seguimiento y localización. 23

4.3 Criterios jurisprudenciales anteriores a la reforma y tratamiento actual 26

5. Seguimiento de dispositivos a través de geolocalización del virus Covid-19 33

5.1 Dispositivos electrónicos de rastreo del Covid-19 a nivel global 33

5.2 Variedad de herramientas eletrónicas a nivel global y el Covid-19 36

5.3 Cómo manejan y obtienen los datos estas aplicaciones 38

5.4 Radar Covid 39

5.4.1 Como funciona Radar Covid 39

5.4.2 Fuente de datos y privacidad de Radar Covid 40

5.4.3 Protección y legislación de los datos utilizados 42

5.5 Programa Datalai en Tenerife 44

6. Concluciones 46

Bibliografía 51

ANEXO I 55

1. Introducción

La sociedad en las últimas décadas ha experimentado numerosas transformaciones, y debido a ello se deben promulgar nueves leyes, así como, actualizar las ya existentes para que no sea profunda la brecha que se genera entre la realidad y su regulación legal.

Vivimos en la "Sociedad de la información y el conocimiento" o "era digital", caracterizada por el trascendental papel que juegan las tecnologías de la información y la comunicación. En el mismo sentido actúa la revolución informática para el desarrollo de la Sociedad de la información y el conocimiento anteriormente mencionada, con particular interés en la transformación que para nuestras vidas ha supuesto la omnipresencia de Internet, debido a la utilización de múltiples dispositivos electrónicos (Smartphones, agendas electrónicas, tablets, ordenadores portátiles, teléfonos móviles…). Dichos avances han provocado la aparición de nuevas conductas y nuevas formas de delinquir que contrastaban con unos textos legales, obsoletos en algunos aspectos, concretamente en lo referente a los instrumentos de investigación tecnológica[1].

La propia Exposición de Motivos de la Ley Orgánica 13/2015, de 5 de octubre, recoge que la irrupción de las nuevas tecnologías no ha podido sustraerse al paso del tiempo, la insuficiencia de un marco normativo concebido para tiempos bien distintos ha obligado al legislador a poner en primer plano esta improrrogable reforma. La información generada por los sistemas de comunicación telemática advierten de las posibilidades al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos. Por lo expuesto,

[1] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, en adelante, LO 13/2015, de 5 de octubre.

surge la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para afrontar una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros[2].

Por todo lo expuestos, ha sido necesario, la regulación de las distintas diligencias de investigación tecnológica que lleva a cabo la LO 13/2015, de 5 de octubre.

Las novedades que se incluyen en la mencionada ley en cuanto a diligencias de investigación tecnológica, son las siguientes:

- La detención y apertura de la correspondencia escrita y telegráfica.
- La interceptación de las comunicaciones telefónicas y telemáticas.
- La incorporación al proceso de datos electrónicos de tráfico o asociados.
- La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos.
- La captación de la imagen en espacios públicos.
- La utilización de dispositivos o medios técnicos de seguimiento y localización.
- El registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

En el presente trabajo se estudian las medidas de investigación recogidas en los artículos 588 quinquies b) y c) de la Ley de Enjuiciamiento Criminal, en adelante LECrim. En concreto, se estudiará la utilización de dispositivos técnicos de seguimiento y de localización que se encuentra regulada en el Capítulo VII.

El ya mencionado Capítulo VII de la LECrim regula *la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización,* pero en el

[2] Díez Ripollés, J L. (24 de abril de 2013). Código Procesal Penal. Recuperado 24 de marzo, 2016, de www.juecesdemocracia.es.

presente estudio, cabe indicar que se excluye el análisis de los dispositivos técnicos de captación de la imagen ya que ha sido objeto de numerosos estudios.

2. Fundamento de la reforma de la LECrim respecto a la investigación tecnológica

A colación del apartado anterior, se expondrá la situación que se vivía en los años que precedieron a la reforma de la LECrim, en los que ya no solo existían dificultades propias en la investigación tecnológica de los delitos, sino que además, se sumaba una LECrim decimonónica, no adaptada a las nuevas necesidades de la investigación criminal, por lo que era necesario acomodar, mediante analogía e interpretación jurisprudencial, la labor de jueces y magistrados, supliendo así, los vacíos legales existentes.

Debido a esta situación se hizo necesaria una reforma de la LECrim que contemplara un nuevo escenario ya que se había instaurado en la sociedad un nuevo tipo de delincuencia.

La reforma llega con la aprobación por el Consejo de Ministros, celebrado el día 5 de diciembre de 2014, de un Anteproyecto de Ley Orgánica de modificación de la LECrim para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas. Este Anteproyecto de ley orgánica se dividió posteriormente en dos proyectos de ley[3]: el Proyecto de Ley de modificación de la LECrim para la agilización de la justicia penal y el fortalecimiento de las garantías procesales, y el Proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

En su Exposición de Motivos se ponía de manifiesto la necesidad de afrontar ciertas

[3] BOE núm. 239, de 6 de octubre de 2015, páginas 90192 a 90219 [BOE-A-2015-10725]

cuestiones que no podían esperar a ser resueltas con la promulgación de un nuevo texto normativo que sustituyera a la Ley de Enjuiciamiento Criminal. Dichas cuestiones eran: *1) la necesidad de establecer disposiciones eficaces de agilización de la justicia penal que eviten dilaciones indebidas; 2) el fortalecimiento de los derechos procesales de conformidad con la exigencias del Derecho de la Unión Europea (UE); 3) la regulación de las medidas de investigación tecnológica; 4) la previsión de un procedimiento de decomiso autónomo; 5) la instauración de la segunda instancia; y, 6) la reforma de la revisión penal.*

Pasado prácticamente un año desde la aprobación por el consejo de ministros del Anteproyecto de Ley Orgánica anteriormente mencionado, se promulgó la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, y la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales (en adelante, Ley 41/2015, de 5 de octubre).

Tal y como expone en su preámbulo, la LO 13/2015, de 5 de octubre, pretende lograr el fortalecimiento de los derechos procesales de conformidad con las exigencias del Derecho de la Unión Europea y la regulación de las medidas de investigación tecnológica en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales garantizados por la Constitución.

Es por ello, que esta Ley Orgánica encabeza una reordenación sistemática de las diligencias de investigación, hasta el momento reguladas en el Título VIII del Libro II de la LECrim, agrupándose todas ellas bajo el epígrafe "*de las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la*

Constitución". Dentro de ese Título VIII se crean diez Capítulos. Los tres primeros recogen las diligencias de investigación ya existentes antes de la reforma, mientras que los otros siete son Capítulos de nueva redacción.

El primero de ellos –arts. 545 a 572- tiene por título "de la entrada y registro en lugar cerrado". El segundo –arts. 573 a 578- "del registro de libros y papeles". El tercero –arts. 579 a 588- "de la detención y apertura de la correspondencia escrita y telegráfica". Respecto de estos tres Capítulos, es preciso hacer referencia a que sólo ha considerado conveniente actualizar la regulación del último Capítulo citado, correspondiente a la detención y apertura de la correspondencia escrita y telegráfica, debido, en gran medida, a la restricción que esas diligencias de investigación suponen respecto de los derechos del art. 18 de la Constitución Española (en adelante, CE) y a la premura impuesta por los tiempos de la legislatura[4].

A los anteriores, se añaden siete Capítulos de nueva redacción, los cuales abarcan desde el Capítulo IV al X. El primero de éstos recoge una serie de "disposiciones comunes" a las que se debe atender en la adopción de cualquiera de las consideradas diligencias de investigación vinculadas con las nuevas tecnologías. Éstas se enumeran en el siguiente orden: "la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos".

Merece el aprobado el simple hecho de que se haya sacado adelante la regulación de estas medidas de investigación, muchas de las cuales, hasta la entrada en vigor de la

[4] GONZÁLEZ-CUÉLLAR SERRANO, N. y MARCHENA GÓMEZ, M., La Reforma de la Ley de Enjuiciamiento Criminal en 2015, Madrid, Castillo de Luna, 2015, p. 173.

norma, permanecían subsumidas en la más absoluta indigencia jurídica, lo que repercutía de forma muy negativa en la investigación y represión de las nuevas formas de criminalidad[5].

Una vez expuesta, de manera general, la incidencia en la LECrim de la reforma, es conveniente abordar, detalladamente, el fundamento de la misma y la forma en que se ha llevado a cabo, así como los antecedentes que han dado lugar a su elaboración.

Insistimos en la naturaleza de la Ley Orgánica 13/15 de 5 de octubre, que incluso, en su preámbulo, de forma explicita, recoge la respuesta acerca del por qué esta modificación ha sido llevada a cabo a través de una ley orgánica y no ordinaria.

Como es sabido esta regulación incide directamente en los artículos 18 y 24 de la CE, Capítulo II, Sección 1, bajo la rúbrica "De los derechos fundamentales y de las libertades públicas". La introducción de cambios jurídicos, sustantivos y procesales, que afectan al ámbito propio de la ley orgánica, desarrollan derechos fundamentales y libertades públicas recogidas en dichos preceptos constitucionales.
A lo largo de los años no ha existido un criterio común que sirviera de fundamento para determinar qué contenidos de la LECrim debían estar sujetos a la reserva de ley orgánica y cuáles debían ser regulados mediante ley ordinaria. Por ello, en muchas ocasiones, preceptos procedimentales fueron elevados de rango, bien en aplicación de lo que el Tribunal Constitucional, en adelante, TC, denomina "materias conexas", o bien, por afectar a leyes que específicamente han de tener naturaleza orgánica.

Por otro lado, la regulación a través de ley orgánica contribuye a favorecer la existencia de un límite en la regulación de estos nuevos medios de investigación

[5] JIMÉNEZ SEGADO, C. y PUCHOL AIGUABELLA, M., "Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección de datos", en Diario La Ley, núm. 8676, 2016, p. 2.

tecnológicos, que puedan afectar, a los derechos fundamentales de los sujetos sometidos a una investigación penal que sin lugar a duda, son titulares de un derecho subjetivo propio, el derecho a la presunción de inocencia. Será necesario buscar un equilibrio entre la facultad del Estado para la persecución de ciertas conductas delictivas y los derechos fundamentales como el derecho a la intimidad o al secreto de las comunicaciones[6].

[6] GONZÁLEZ-MONTES SÁNCHEZ, J.L., "Reflexiones sobre el Proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas", en Revista Electrónica de Ciencia Penal y Criminología, núm. 17- 06, 2015, p. 21.

3. Disposiciones comunes a las medidas de investigación tecnológicas

Estas disposiciones comunes se encuentran reguladas en el Capítulo IV del Título VIII del Libro II, introducido por el apartado trece del art. único de la LO 13/2015, de 5 de octubre.

3.1 Principios rectores

Para poder acordar las medidas de investigación tecnológica se precisa que medie autorización judicial, exigiendo que la misma se sujete plenamente a los principios rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

En relación con lo anterior, los criterios que deben inspirar la autorización o no de las medidas vienen establecidos en la ley, bajo la denominación de "principios rectores" que son comunes a todas estas medidas, concretamente en el art. 588 bis a 1º LECrim, y los supedita a que se esté llevando a cabo la instrucción de una causa penal y siempre que medie autorización judicial. Se enumeran en los art. 588 bis a 2º LECrim y siguientes como principios rectores[7]:

El principio de especialidad implica que la medida debe estar relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva. En relación con este principio hay que destacar que, la utilización de la información obtenida en un proceso penal distinto y para los

[7] RAYÓN BALLESTEROS, M, C, "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015", en Anuario Jurídico y Económico Escurialense, LII (2019) 179-204 / ISSN: 1133-3677.

descubrimientos casuales, hay que aplicar lo dispuesto en el art. 579 bis de la LECrim, de esta forma se tendrá que expedir testimonio de particulares[8] para que sea incorporado al proceso penal por el delito diferente al investigado[9].

En conclusión la intervención no puede autorizarse de manera genérica, sino que en base a su carácter debe darse para el delito en concreto no pudiendo darse para prevenir o descubrir delitos sin una base objetiva y fundamentada.

El principio de idoneidad se refiere a los aspectos concretos de la medida que se acuerda judicialmente, desde un punto de vista tanto objetivo como subjetivo y su duración. En cuanto a la extensión subjetiva de la medida hay que hacer referencia al art. 588 bis h) que establece que se pueden acordar medidas de investigación *"aun cuando afecten a terceras personas en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas"*. La extensión objetiva la medida se refiere a la concreta autorización judicial que la acuerda. Y la duración de la medida deberá prorrogarse el tiempo necesario para alcanzar los fines de la investigación sin necesidad de alcanzar los plazos máximos establecidos legalmente[10].

[8] Este testimonio deberá incluir los particulares necesarios para autorizar la injerencia, sobre todo lo relativo a la solicitud inicial de la medida, la resolución judicial que la acuerda y todas las peticiones y resoluciones de prórroga recaídas en el proceso de origen. La medida puede continuar con la autorización del juez que conozca de este otro proceso.

[9] Para mayor aclaración, consultar la Instrucción 2/2017, de 28 de abril, sobre procesos incoados a raíz de la deducción de testimonios de una causa principal. Doctrina de la Fiscalía General del Estado.

[10] RAYÓN BALLESTEROS, M. C., "medidas de investigación tecnológicas en el proceso penal: (…)", op. cit, pag 8.

El principios de excepcionalidad y necesidad, solo podrá acordarse la medida correspondiente cuando no estén a disposición de la investigación otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.

El principio de proporcionalidad exige la ponderación entre el sacrificio de los derechos e intereses afectados por la medida de investigación y el beneficio que se derive para el interés público y de terceros con su adopción, establece los elementos que habrán de valorarse a la hora de llevar a cabo tal ponderación, haciendo referencia a la gravedad del hecho, su trascendencia social, el ámbito tecnológico de su producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho fundamental[11].

3.2 Procedimiento para la solicitud y autorización judicial de la medida de investigación tecnológica.

La medida podrá adaptarse de oficio, a instancia del Ministerio Fiscal (en adelante, MF), o a instancia de la Policía Judicial (en adelante PJ).

[11] LÓPEZ CAUSAPÉ, E., "Las medidas de investigación tecnológica en la ley de enjuiciamiento criminal", Boletín Digital Penal, Asociación Judicial Francisco de Vitoria, julio, 2016.

El Art. 588 bis b) LECrim recoge los requisitos que han de concurrir en la solicitud al Juez Instructor de la adopción de la medida:

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

2º) La exposición de las razones que justifiquen la necesidad de la medida y los indicios de criminalidad puestos de manifiesto durante la investigación previa.

3º) Los datos de identificación del investigado y de los medios de comunicación empleados.

4º) La extensión de la medida especificando su contenido.

5º) La unidad investigadora de la Policía Judicial que vaya a hacerse cargo de la intervención.

6º) La forma de ejecución de la medida.

7º) La duración de la medida solicitada.

8º) El sujeto obligado a llevar a cabo la medida en caso de ser conocido".

Una vez solicitada la medida el Juez de Instrucción oirá al MF y autorizará o denegará la misma mediante auto motivado dictado en el plazo máximo de veinticuatro horas desde que se presente la solicitud[12].

[12] Este plazo de 24 horas puede ser interrumpido por el juez si requiere una ampliación o aclaración de la solicitud para resolver sobre el cumplimiento de alguno de los requisitos expresados (art. 588 bis c 1º LECrim).

3.3 Duración de la medida

Respecto a la duración de las medidas, el art. 588 bis e) LECrim recoge que se especificará, caso a caso, para cada una de ellas si bien *"no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos"*.

Así mismo, las medidas podrán ser prorrogadas si persisten las causas que la motivaron, y se necesitara nuevamente dictar un auto motivado por el juez competente, bien de oficio o bien previa petición razonada del solicitante. De lo contrario, transcurrido el plazo por el que resultó concedida la medida, sin haberse acordado su prórroga, conllevará la consecuencia automática del cese de la misma[13]. Del mismo modo, cabe mencionar que para algunas medidas se contemplan otros límites de duración:

-Para los registros remotos sobre equipos informáticos: plazo máximo un mes con posible prórrogas por periodos sucesivos de un mes con un máximo de tres meses.

-Para la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos: no obedece a ninguna limitación temporal, ya que se refiere a encuentros precisos y concretos del investigado.

-Para la interceptación de las comunicaciones telefónicas y telemáticas y la utilización de dispositivos técnicos de seguimiento y de localización: tiempo máximo de tres meses con posibles prórrogas por periodos sucesivos de tres meses hasta un máximo, de dieciocho meses.

---

13 *"La solicitud de prórroga se dirigirá por el Ministerio Fiscal o la Policía Judicial al juez competente con la antelación suficiente a la expiración del plazo concedido. Deberá incluir en todo caso: a) Un informe detallado del resultado de la medida; b) Las razones que justifiquen la continuación de la misma. Presentada la solicitud el juez resolverá sobre el fin de la medida o su prórroga mediante auto motivado. Antes de dictar la resolución podrá solicitar aclaraciones o mayor información. Concedida la prórroga, su cómputo se iniciará desde la fecha de expiración del plazo de la medida acordada"* (art. 588 bis f LECrim).

3.4 Control judicial de la medida de investigación tecnológica.

Respecto al control de la medida de investigación tecnológica introducida, el art. 588 bis g) LECrim indica que el juez de instrucción deberá ser informado por la PJ del desarrollo y los resultados de la medida, en la forma y con la periodicidad que el mismo establezca y, siempre en todo caso, cuando se ponga fin a la medida.

A lo largo de la vigencia de la medida los resultados que se obtengan se van incorporando al proceso mediante los correspondientes soportes (grabaciones, captaciones, etc.), conservándose en una pieza separada y secreta para las partes, todo ello, con el propósito de no perjudicar el resultado obtenido de la investigación. En cuanto se decrete el cese de la medida, se levanta el secreto y se entrega a las partes copia de las grabaciones, transcripciones, captaciones.

3.5 Deber de colaboración

La LECrim exige el deber de colaboración de todas las empresas y sujetos que proporcionan o gestionan los medios tecnológicos a que se refieran las medidas acordadas, con el fin de facilitar la ejecución de las medidas de investigación, ya que son indispensable para su interceptación. Dicho deber de colaboración se exige a toda persona que conozca el funcionamiento del sistema informático o medidas aplicadas para proteger los datos a que se refiere la investigación y a su vez, se extiende también a los prestadores de servicios y los titulares y administradores de los sistemas informáticos.

La referida colaboración puede instarse tanto por el MF como por la PJ, antes de obtener la autorización judicial de las medidas, siempre con el propósito de conservar y/o proteger los datos de que dispongan, hasta que finalmente el juez otorgue el acceso a los mismos[14].

3.6 Cese de la medida y destrucción de los registros obtenidos

El juez acordará el cese de la medida de investigación tal y como dispone el art. 588 bis j) cuando se den alguna de las siguientes circunstancias:

- Una vez conste que con la implantación de la medida, no se estén obteniendo los resultados pretendidos,

- Desaparezcan las circunstancias que justificaron su adopción.

- Y, siempre que, se haya transcurrido el plazo para el que hubiera sido autorizada.

Una vez cesa la medida, se comunicará a la personas o personas afectadas por la misma y se les facilitará copia de los resultados obtenidos si así lo solicitan.

Tal y como recoge el art. 588 bis k) LECrim, una vez que se ponga término al proceso penal mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos

[14] RAYÓN BALLESTEROS, M. C., "medidas de investigación tecnológicas en el proceso penal: (…)", op. cit, pag 8.

utilizados en la ejecución de la medida. Así mismo, se conservará una copia bajo custodia del Letrado de la Administración de Justicia.

4. Utilización de dispositivos técnicos de seguimiento y localización

Se entiende como seguimiento remoto o tecnológico la técnica policial consistente en la colocación de un dispositivo, capaz de facilitar el posicionamiento a otro dispositivo manejado, permitiendo hacer un seguimiento y localización del mismo. Se trata de cualquier artificio técnico de geolocalización que tenga una relación directa o indirecta con una persona y por lo tanto pueda afectar al derecho a la intimidad.

Es una medida de investigación, que consiste en la utilización de dispositivos técnicos de seguimiento y localización en la investigación de comportamientos delictivos. Esta diligencia requiere autorización judicial, que deberá especificar que medio técnico va a ser utilizado. La medida podrá ser autorizada por el Juez competente siempre y cuando concurran acreditadas razones de necesidad y resulte proporcionada, como se observa, siempre inspirada en el principio de necesidad y proporcionalidad, dada la posible incidencia de la medida en los derechos fundamentales del investigado (apartados 1 y 2 del artículo 588. quiquies. b LECrim).

Lo expuesto anteriormente, goza de una excepción a la regla general, ya que hasta antes de la reforma de la LECrim, competía únicamente a las Fuerzas y Cuerpos de Seguridad del Estado[15] la colocación de los dispositivos de localización y seguimiento, sin la previa autorización judicial *ex* art. 588 quinquies b) LECrim apartado 4. En este caso, el Juez debería ratificar la medida o cesarla, en el plazo máximo de 24 horas posterior a su conocimiento.

[15] Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

4.1 Clases de dispositivos técnicos de seguimiento y localización.

La geolocalización puede realizarse a través de:

Dispositivos técnicos basados en sistemas de posicionamiento global (GPS, GLONASS, etc.) o bien, a través de los datos electrónicos asociados a sistemas de comunicación telefónica.

Los sistemas de posicionamiento global (en adelante, GPS) que son los más utilizados, reciben información, a través de canales abiertos de comunicación, de una red de satélites que proporcionan datos de manera constante sobre la posición geográfica de cualquier dispositivo que conecte con ellos.

Este método de geolocalización ha sido perfeccionado en los últimos años a través de un aumento de los datos que proporcionan los propios satélites o mediante servicios de valor añadido generalmente suministrados por organismos públicos a través de:

1. Receptores A-GPS o GPS, conocidos como balizas, que complementan los datos propios del sistema GPS con otros datos proporcionados por la red de telefonía móvil con fin de conocer la ubicación del sujeto.

2. Sistemas de radiofrecuencia que permiten la identificación de objetos o personas que se encuentran a cierta distancia sin necesidad de mantener contacto con los mismos. Para ello, es imprescindible incorporar al sujeto investigado, un microchip que lleva incorporado una micro-antena de radio y que por tanto, permite rastrear la señal del dispositivo.

*"*El posicionamiento a través de los datos asociados a sistemas de comunicación telefónica se consigue gracias al llamado sistema global para las comunicaciones móviles *"* (GSM 3, 4 y 5 G). Ello se denomina localización GSM.

Estos dispositivos permiten conocer la posición del investigado gracias a los datos que el sistema de telefonía móvil puede obtener de las estaciones BTS[16] o redes wifi, así como de las posibilidades que le ofrece su acceso a Internet. Es un servicio proporcionado por las empresas de telecomunicaciones que permite determinar la posición aproximada de un teléfono móvil gracias a su constante conexión con las estaciones BTS. Estos datos de geolocalización deben ser considerados datos asociados a las comunicaciones telefónicas, aunque no datos de tráfico, ya que pueden generarse independientemente del mantenimiento o no de una comunicación.

En relación con lo expuesto, determinamos que son dos los sistemas de geolocalización susceptibles de ser utilizados para el seguimiento y localización de un investigado: "El primero, consistente en el uso de un dispositivo GPS o similar, controlado por la Policía Judicial, que se instalara en un vehículo o cualquier otro objeto que pudiera llevar consigo el investigado, permitiendo de este modo vigilar sus desplazamientos o ubicaciones; el segundo, mediante la obtención de los datos de localización GSM que pudiera generar el dispositivo de telefonía móvil del investigado, datos éstos en poder de la compañía de telecomunicaciones. En el primer caso estaríamos en presencia de lo que el art. 588 quinquies b llama

[16] Una estación base o BTS (Base Transceiver Station) es un elemento de red de comunicaciones móviles fundamental, quizá el más importante, se trata de un equipamiento fijo distribuido por el territorio terrestre para cubrir el área a la que se pretende prestar el servicio de cobertura.

dispositivos técnicos de seguimiento y localización, mientras que, en el segundo, se trataría de lo que denomina medios técnicos de seguimiento y localización"[17].

Por ello, cuando se trate de dispositivos GPS, será la PJ la que directamente controle y obtenga los datos de posicionamiento que genere el dispositivo y, por lo tanto, a ella deberá dirigir el Juez de Instrucción el oficio acordando la medida. En la localización GSM, por el contrario, se deberá dirigirse a las compañías de telecomunicaciones y, en ambos casos, con sujeción a las prescripciones contenidas en el art. 588 quinquies b y c LECrim. De este último supuesto, sin embargo, se exceptuarán las situaciones en las que la incorporación al proceso de los datos asociados haya sido acordada en una resolución judicial de intervención de las comunicaciones telefónicas, en las que resultarán de aplicación las disposiciones contenidas en el Capítulo V LECrim, referidas a la interceptación de comunicaciones telefónicas y telemáticas.

Cabe mencionar un supuesto que se escapa a esta regulación, que será el que se plantee cuando se trate de obtener datos de geolocalización, no en tiempo real, sino de fechas anteriores. En estos casos resultarán de aplicación los arts. 588 sexies a y siguientes LECrim, cuando se pretenda el registro de dispositivos GPS hallados en poder del investigado, o el art. 588 ter j LECrim, cuando se trate de obtener datos asociados a comunicaciones telefónicas que obren en los archivos automatizados de los prestadores de servicios o personas que faciliten comunicaciones en cumplimiento de la legislación sobre retención de datos relativos a comunicaciones electrónicas[18].

---

[17] Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado (FGE), sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización. - BOE, 22-03-2019.

[18] Idem, pag 16.

4.2 Posibilidad de afectar derechos fundamentales por la utilización de dispositivos técnicos de seguimiento y localización

El uso de dispositivos técnicos de seguimiento y localización puede suponer una limitación del derecho fundamental a la intimidad (art. 18.1 CE). Por ello, la monitorización del vehículo del sujeto investigado mediante un dispositivo técnico de geolocalización, permite conocer aspectos de su intimidad, que entran en el "ámbito reservado de la vida de las personas excluido del conocimiento de terceros" (SSTC n.º 10/2002, de 17 de enero; 127/2003, de 30 de junio y 189/2004, de 2 de noviembre).

Respecto a lo expuesto se entiende por,

Derecho a la intimidad, aquel que se relaciona con lo más íntimo de la persona, en todos los ámbitos de la vida, ya sea el familiar o el personal propio. Se encuentra ligado con la esfera más reservada de la vida personal, e incluso, se reconoce aquellas personas que tienen la consideración de "personajes públicos"[19].

Del mismo modo, el art. 8 de "Derecho al respeto a la vida privada y familiar" del Convenio de Protección de los Derechos Humanos y Libertades Fundamentales de 1979, corrobora lo ya expuesto, afirmando que:

"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

[19] López Guerra, L, (1994). Introducción al Derecho Constitucional. Barcelona: Tirant lo Blanch. págs 23-40.

2. 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."

Derecho al honor, no existen definiciones del concepto de honor en textos legales, pero de las múltiples Sentencias del TC destacamos la nº 139/1995, que recoge la doctrina sentada por dicho TC sobre su concepto y denominador común de la defensa del mismo

"A pesar de la imposibilidad de elaborar un concepto incontrovertible y permanente sobre el derecho al honor, ello no ha impedido, acudiendo al Diccionario de la Real Academia Española, asociar el concepto de honor a la buena reputación (concepto utilizado por el Convenio de Roma), la cual – como la fama y aún la honra – consisten en la opinión que las gentes tienen de una persona, buena o positiva si no van acompañadas de adjetivo alguno. Así como este anverso de la noción se da por sabido en las normas, éstas, en cambio, intentan aprehender el reverso, el deshonor, la deshonra o difamación, lo difamante. El denominador común de todos los ataques e intromisiones ilegítimas en el ámbito de protección de este derecho es el desmerecimiento en la consideración ajena (art. 7.7 L.O. 1/1982) como consecuencia de expresiones proferidas en descrédito o menosprecio de alguien o que fueron tenidas en el concepto público por afrentosas".

Tras lo expuesto, surge la siguiente cuestión ¿Cuándo se considera ilegal la utilización de dispositivos de localización o seguimiento en una investigación?

La *STC 123/2002, de 20 de mayo* en su Fundamento Jurídico 4 (en adelante FJ), responde de la siguiente manera: "…para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad es necesario constatar si cumple estos tres requisitos: a) si la medida acordada puede conseguir el objetivo propuesto (juicio de idoneidad); b) si es necesaria en el sentido de que no exista otro medio más moderado para conseguir el fin propuesto con igual eficacia (juicio de necesidad); c) si la medida es ponderada o equilibrada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)". Y en fecha más reciente se ha pronunciado la STC 142/2012, de 2 de julio en su FJ 2.

Por tanto, la doctrina constitucional ha consagrado una serie de principios rectores para establecer unos límites en la adopción de esta diligencia de investigación, estos límites se contemplan en el art. 588 bis a) LECrim, ya referidos en el apartado 3[20]. Los principios que el artículo acuña son: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad en la medida ya explicados en el apartado anterior. Se trata de presupuestos constitucionales de obligado cumplimiento que, en el caso de ser vulnerados, dará lugar a la ilicitud de la prueba conforme el art. 11.1 de la Ley Orgánica del Poder Judicial (en adelante, LOPJ) [21].

De los principios reseñados, el principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. Por lo tanto, no podrán

[20] Teniendo en cuenta estos principios, se autoriza de forma expresa la posibilidad de restringir estos derechos fundamentales siempre que cumplan una finalidad legítima y que a consecuencia de esta limitación se obtenga un interés socialmente relevante.

[21] "*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"* (art.11.1 LOPJ).

autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.

"A pesar de la limitación de la intimidad que a través de los dispositivos técnicos de seguimiento y localización se produce, se trata, por regla general, de intromisiones de baja intensidad. La citada STEDH de 2 de septiembre de 2010 pone de manifiesto, incluso, que las vigilancias y seguimientos llevados a cabo a través de estos dispositivos suponen una intromisión en la vida privada de menor intensidad que la vigilancia visual o acústica llevada a cabo directamente por agentes policiales, al poder complementarse de esta última forma el dato de la geolocalización con otros que se perciben por la vista o el oído. Esta circunstancia hace que el propio TEDH rebaje las exigencias necesarias para la utilización de esta técnica de investigación en relación con otras, como las intervenciones telefónicas, haciendo depender casi en exclusiva la legalidad de su uso del juicio de proporcionalidad"[22] .

4.3 Criterios jurisprudenciales anteriores a la reforma y tratamiento actual

En este apartado se estudiaran los pronunciamientos jurisprudenciales respecto a esta medida de investigación tecnológica, dispositivos técnicos de seguimiento y localización, anteriores a la reforma operada por la LO 13/2015 de 5 de octubre, con la finalidad de observar la práctica policial cuando no se apoyaba en una norma expresa que le habilitara y la colisión con el derecho a la intimidad resultaba evidente, como ya se ha mencionado en el apartado anterior.

22 Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado (FGE), sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización. - BOE, 22-03-2019.

La utilización de esta medida era considerada por el Tribunal Supremo (en adelante, TS) como una diligencia de investigación legítima desde la función constitucional, restrictiva de derechos fundamentales. La PJ se valía de estas medidas en casos de urgente necesidad, sin perjuicio, de poner en conocimiento de la autoridad judicial competente, el establecimiento de la misma y las causas que las motivaron. Hay que insistir en que les competía a las Fuerzas y Cuerpos de Seguridad del Estado la decisión de valerse de dichos dispositivos sin previa autorización judicial.

Por otro lado, el TS convalidó su utilización, por vía jurisprudencial mediante la aplicación analógica de los preceptos relativos a la "detención y apertura de la correspondencia escrita y telegráfica" –art. 579 y ss LECrim-.

Se han seleccionado ciertos pronunciamientos jurisprudenciales, relacionado con lo que estudia en el presente trabajo, para de esta forma, explicar algunas cuestiones.

La sentencia (en adelante, STS) nº 562/2007 de TS, Sala 2ª, (de lo Penal), 22 de Junio de 2007. En la STS, se denuncia la vulneración del derecho fundamental al proceso debido y a la intimidad que se concretan en el hecho de haber colocado una baliza de seguimiento sin autorización judicial. El propio tribunal desmiente lo expuesto por la parte recurrente y establece que el dispositivo de localización colocado permitió a los agentes de investigación el seguimiento por mar de la embarcación dado que existían fundadas sospechas de su dedicación al tráfico de drogas. La colocación de esa baliza, en los exteriores del barco, no precisó ninguna injerencia en ámbitos de intimidad constitucionalmente protegidos. Y finaliza exponiendo que se trata de una 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 requeriría la intervención judicial.

En la STS nº 523/2008 de TS, Sala 2ª, de lo Penal, 11 de Julio de 2008, nuevamente los condenados alegaron que se vulneró su derecho a la intimidad al colocarse una baliza de seguimiento en la embarcación objeto de la investigación, el tribunal en el submotivo 2 b) desestima sus alegaciones de la siguiente manera: *"Concierne a la vulneración del derecho a la "intimidad de domicilio", reconocido en el art. 18.2 CE. Para lo que se aduce que en el puente del DIRECCION000 fue colocado por el SVA una baliza de seguimiento y localización.*

En primer lugar, 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 LECr.. Atendidos los documentos de los folios 3510 a 3515 y las declaraciones en el juicio oral de los funcionarios del Servicio de Vigilancia Aduanera con números terminados en 0035 y 268 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 ingerencia en las conversaciones o mensajes de los investigados."

Una vez más, el tribunal no considera ilegal la utilización de estos medios de localización y seguimiento.

La STS nº 789/2013 del TS Sala de lo Penal, de 5 de Noviembre de 2013 sigue la línea de las anteriores al expresar en su FJ 11, *"...que el alegado motivo de violación de precepto constitucional, art.18, dado que como se reconoció en el acto del juicio la localización de la embarcación fue posible por medios técnicos, en concreto GPS, empleados por los miembros de Vigilancia Aduanera que sabían las coordenadas exactas a que tenían que acudir para interceptarla, vulneraría su derecho a la intimidad, citando en su apoyo la STEDH caso Uzun contra Alemania, impugnación*

que debe ser desestimada…siendo así no se aprecia violación alguna del derecho a la intimidad.

El uso de radiotransmisores (balizas de seguimiento GPS), para la localización de embarcaciones en alta mar por la policía no vulnera el derecho fundamental al secreto de las comunicaciones o supone una injerencia excesiva sobre el derecho fundamental a la intimidad a los efectos de exigir un control jurisdiccional previo y una ponderación sobre dicha afectación constitucional.

Para esta Sala Segunda Tribunal Supremo la ausencia de relevancia constitucional se deriva de que se trata de "diligencias de investigación legitimas desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiera en su derecho fundamental que requeriría intervención judicial" (SSTS. 22.6.2007, 11.7.2008 y 19.12.2008), e incluso la sentencia TEDH citada en el recurso, caso Uzun contra Alemania de 2.9.2010, también precisó que la vigilancia GPS, por su propia naturaleza debe distinguirse de otros métodos de seguimiento acústico o visual que, por regla general, son más susceptibles de interferir en el derecho de la persona al respeto de su vida privada, porque revelan unas informaciones sobre la conducta de una persona, sus operaciones o sus sentimientos".

El siguiente auto del Tribunal Superior de Justicia de Cataluña de la Sala de lo Penal 211/2014, resuelve un recurso de apelación interpuesto por la defensa de un acusado contra un auto de 10 de diciembre de 2013, que rechazaba una cuestión previa formulada en un proceso penal ante tribunal de jurado, en virtud de la cual se solicitaba la nulidad de la diligencia de instalación de un dispositivo GPS por parte de la fuerza policial en el vehículo habitualmente utilizado por el acusado, sin autorización judicial, por entender que se había vulnerado el derecho a la intimidad,

recogido en el artículo 18 de la CE, en relación y concordancia con lo dispuesto en los artículos 7 y 8 de la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. La sentencia expone lo siguiente: *"Por tanto, debe concluirse que, en el presente caso, el seguimiento del turismo del acusado mediante baliza o GPS, debe reputarse proporcional y necesario a los objetivos legítimos perseguidos, máxime cuando, como antes se ha indicado, existía una investigación judicial ya abierta, con la finalidad de descubrir al culpable de la comisión de unos delitos graves, en la cual la policía actuante venía solicitando autorización, de forma reiterada y constante, para la realización de todas las diligencias y medidas que podían causar alguna injerencia al sospechoso, y de cuyos resultados, además, se iba informando y dando cuenta a la autoridad judicial. En definitiva, no se estima que en el supuesto analizado se haya vulnerado el derecho a la intimidad personal previsto en el artículo 18 de la CE ni se haya infringido lo dispuesto en los citados artículos 7 y 8 de la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor , a la intimidad personal y familiar y a la propia imagen, por lo que debe rechazarse la solicitud de nulidad tanto de la diligencia de instalación por parte de la policía de un dispositivo GPS en el vehículo habitualmente utilizado por el acusado, como de las periciales y documentales derivadas de aquélla".*

Tras los diferentes pronunciamientos jurisprudenciales analizados se llega a la conclusión de que los Tribunales respaldaban ya la utilización de los dispositivos de localización y seguimiento, antes de la reforma de la LO 13/2015 de 5 de octubre, considerando estas medidas de investigación, propias de las funciones asignadas a la policía judicial, siempre que dichas decisiones respondieran a las principios de proporcionalidad y necesidad exigidos.

A diferencia de lo recogido en las anteriores resoluciones en las que aún no había entrado en vigor la reforma de la LECrim, se dicta la STS 141/2020, de 13 de mayo que se pronuncia sobre la validez de la prueba obtenida mediante la colocación por los Agentes de Policía de un dispositivo GPS en el vehículo del investigado, a tenor de lo previsto en el artículo 588 quinquies b) LECrim. La STS estima el recurso interpuesto por la defensa por vulneración del derecho fundamental a la intimidad del art.18 CE, casando y anulando la sentencia del Tribunal de instancia y dictando otra en su lugar donde absuelven al acusado del delito de tráfico de drogas por el que había sido condenado.

En este supuesto los Agentes habían colocado un dispositivo GPS en el vehículo del acusado que posteriormente les permitió detenerle portando 100 gramos de cocaína. El Auto que autorizó la colación de este dispositivo se basó en tres indicios: 1) una confidencia anónima; 2) la existencia de antecedentes policiales por tráfico de drogas; 3) la constatación, a través de las cámaras de la DGT, que hacía viajes entre dos localidades.

Tras la reforma introducida por la LO 13/2015 no cabe duda que la utilización de dispositivos de localización y seguimiento tiene una incidencia directa en la intimidad y es necesario subordinar la legitimidad del acto de intromisión a la previa autorización judicial. Esto obliga a rectificar pautas de actuación policial, hasta ahora validadas por la jurisprudencia de esta Sala. En este punto, nos recuerda la STS que en principio conocer la localización del lugar exacto en que se halla el investigado se limita a otorgar una ventaja operativa a los investigadores. Pero también existen espacios de ubicación que pierden su aparente neutralidad para ofrecer una radiografía ideológica, religiosa, sanitaria o sobre preferencias de la vida sexual del investigado, etc, afectando al núcleo duro de la intimidad.

Es preciso reconocer que, a diferencia de lo que acontece con otras medidas de injerencia, la nueva regulación no menciona la exigencia de que el acto jurisdiccional habilitante sea el resultado de un juicio de proporcionalidad. Sin embargo, los principios de proporcionalidad, necesidad y excepcionalidad siguen actuando como presupuestos de legitimidad, cuya concurrencia ha de quedar expresamente reflejada en la resolución judicial habilitante.
Entiende esta STS que no se puede aceptar como norma general que esos tres elementos indiciarios sean suficientes para arrebatar a cualquier ciudadano el inicial blindaje que le proporciona su derecho a la intimidad.

La información confidencial, es decir, aquella cuyo transmitente no está necesariamente identificado, debe ser objeto de juicio de ponderación reforzado, en el que su destinatario valore su verosimilitud, credibilidad y suficiencia para la incoación del proceso penal. Por ello una confidencia anónima, a la que sigue la simple constatación de unos viajes en automóvil y la existencia de antecedentes policiales, no puede justificar una invasión estatal de la intimidad, ni siquiera con la cobertura de una resolución judicial.

Se vulnera así el derecho a la intimidad del investigado (art.18.1 ce) y se incurre en la prohibición de valorar prueba ilícita, en los términos del art. 11 de la LOPJ. El vacío probatorio que sigue a la declaración de nulidad de esa prueba, provoca la absolución del acusado.

5. Seguimiento y localización del virus Covid-19

5.1Dispositivos electrónicos de rastreo del Covid-19 a nivel global

Actualmente la situación generada por la pandemia del virus Covid-19 ha requerido un esfuerzo por controlar la expansión de la transmisión de la enfermedad lo que, a su vez, supone un mayor control de las personas contagiadas y sus movimientos. La tecnología en éste aspecto ha supuesto un factor clave a través de la creación de herramientas que den información sobre la proximidad física de la sociedad, que ha sido un elemento clave para controlar los contagios.

Todo este sistema se establece sobre una base ideológica que entiende, que la mayoría de las personas llevan consigo un teléfono inteligente, por lo que se han centrado en la creación de aplicaciones de seguimiento que puedan utilizarse en éstos dispositivos móviles. La mayoría de éstas aplicaciones son patrocinadas por los gobiernos y utilizan variedad de métodos diferentes para su propósito, así el sistema de bluetooth[23] o el sistema de posicionamiento global (en adelante, GPS), entre otros medios. Cabe decir que no todas cumplen una política transparente de privacidad con los usuarios, por ello, se puede afirmar, que la línea que separa la privacidad y las estrategias de control es cada vez más delgada,

Hasta la fecha existen dos métodos principales para rastrear la proximidad física de los usuarios. Uno de ellos, es el GPS, que utiliza la radionavegación por satélite para aproximar la ubicación de los usuarios y saber si éstas son próximas o no. El

[23] El Bluetooth es un protocolo de comunicaciones que sirve para la transmisión inalámbrica de datos y voz entre diferentes dispositivos que se hallan a corta distancia, dentro de un radio de alcance que, generalmente, es de doce metros.

segundo método y el más destacado, es el uso del bluetooth y la intensidad de la señal para identificar la cercanía de los individuos permitiendo que los dispositivos muestren la proximidad, no la ubicación real, por lo que se entiende menos invasiva en el ámbito de la privacidad de los usuarios. Otros programas usan una combinación de los dos métodos anteriores (bluetooth y GPS) y existen otros que, incluso, usan el seguimiento de ubicación basado en la red, pero éstos presentan graves inconvenientes en el ámbito de la privacidad.

El sistema más utilizado en las aplicaciones de rastreo, como ya se ha mencionado anteriormente, es el bluetooth, que ofrece mayor protección de la privacidad. Sin embargo, presenta un problema, pero antes de explicarlo es pertinente conocer el término: visibilidad de Bluetooth, que se refiere simplemente a si otros dispositivos pueden descubrir su equipo al buscar dispositivos Bluetooth. Cuando la visibilidad de Bluetooth está activada y el panel de Bluetooth está abierto, su equipo informará al resto de dispositivos que estén al alcance, permitiéndoles que se intenten conectar a su equipo. Hecho este inciso, cabe decir, que el modo "descubrir" de Bluetooth no está habilitado mientras un teléfono está bloqueado y la aplicación que lo solicita no sea primaria[24].

En las primeras versiones de aplicaciones como BlueTrace[25], la solución del gobierno de Singapur para el rastreo del Covid-19, dependía de que sus usuarios

[24] Se denominan aplicaciones primarias a aquellas que viene predeterminadas e instaladas en el teléfono inteligente.

[25] Aplicación de código abierto (el software de código abierto es aquel distribuido bajo una licencia que permite su uso, modificación y redistribución), que facilita el rastreo de contactos digitales de los usuarios para detener la propagación de la pandemia de COVID-19. Desarrollado inicialmente por el Gobierno de Singapur, BlueTrace impulsa el rastreo de contactos para la aplicación TraceTogether.

mantuvieran sus teléfonos desbloqueados. La aplicación en fase beta del servicio nacional público de salud del Reino Unido (en adelante, NHS), tenía una solución única para esto, al menos para Android, pero parece que los límites implementados por la marca Apple en iOS[26] manisfiestan que esto era algo inalcanzable y ha requerido que los desarrolladores trabajen con la interfaz de programación de aplicaciones (en adelante, API [27]), y notificaciones de exposición de Apple y Google.

La solución conjunta de Google y Apple, es la API oficial de notificaciones de exposición, ya que preserva la privacidad y proporciona un método de uso de "Bluetooth Low Energy" y criptografía[28] para proporcionar una infraestructura de seguimiento de contactos. El uso de la API está limitado a las autoridades de salud pública y el acceso solo se otorga cuando se cumplen criterios específicos sobre privacidad, seguridad y datos. Sin embargo, esta API es solo una parte de la solución que una aplicación necesita para ofrecer la funcionalidad necesaria. Si una aplicación solicita información personal, ya sea directamente o por otros métodos, podría hacer que esta solución, respetuosa con la privacidad, sea cuestionable. Lo expuesto, puede terminar creando en los usuarios una falsa sensación de seguridad.

Esta solución creada por Google y Apple se suma a otros ocho frameworks que han sido creados desde el comienzo de la pandemia. Estos frameworks han sido creados

[26] Es un sistema operativo móvil de la multinacional Apple Inc. Originalmente desarrollado para el iPhone, después se ha usado en dispositivos como el iPod touch y el iPad.

[27] Supone un conjunto de reglas y especificaciones que las aplicaciones pueden seguir para comunicarse entre ellas: sirviendo de interfaz entre programas diferentes.

[28] Técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados

de forma paralela por un conjunto de compañías tecnológicas, organizaciones de privacidad, la academia y gobiernos[29].

5.2 Variedad de herramientas electrónicas a nivel global y el Covid-19

Cada país ha adoptado, bien un framework propio, o bien uno de los nueve que se han desarrollado, cada uno de ellos proporciona un equilibrio diferente entre eficiencia y privacidad. El uso de los diferentes frameworks puede causar problemas de distinta índole, por ejemplo, la mayoría de los países europeos han adoptado la API de Notificación de Exposición de Google y Apple, mientras que Francia no ha procesado los datos de manera centralizada[30]. Desde ésta perspectiva, ha sido imposible, que antes de las apertura de fronteras, existiera una sincronización efectiva entre las aplicaciones de los distintos países.

Estas herramientas de autodiagnóstico están proliferando a nivel mundial a un ritmo vertiginoso. Según diversos estudios consultados, en Corea del Sur ha tenido más de un millón de descargas. De tal manera que, la sociedad coreana ha conseguido aislar a los infectados, reduciendo así la propagación del virus. Sin embargo, restricciones

[29] La palabra Framework es la combinación de dos palabras, es decir, Marco (frame) y Trabajo (work). Esto significa que ya se ha diseñado un marco y que el desarrollador debe funcionar en ese marco para cumplir con los requisitos de su proyecto. Es solo una herramienta que ayuda al desarrollador a codificar mejor y más rápido.

[30] Los términos descentralizado y centralizado se usan con frecuencia para representar visualmente dónde se procesan y almacenan los datos recopilados por una aplicación de rastreo de contactos; dando la percepción de que la centralización crea un mayor riesgo para la privacidad. Esto puede no ser cierto, ya que hay diseños que utilizan un enfoque centralizado pero que potencialmente le brindan al usuario de la aplicación el nivel deseado de privacidad. El problema subyacente es si el uso de los datos puede ser mal utilizado; es decir, si se revela la identidad del usuario o si esta información puede obtenerse fácilmente.

en materia de protección de datos en Europa, más garantista con el ciudadano, dificulta la implantación de una herramienta estandarizada en todos los territorios porque puede implicar una invasión de la privacidad, aunque los primeros proyectos se han empezado a aplicar de manera anónima y de forma voluntaria.

Debido a lo expuesto anteriormente, se crea Covid Tracing Tracker (rastreador de rastreadores del Covid), con el fin de realizar un seguimiento de aquellas aplicaciones que a su vez rastrean nuestra posición. De esta manera, Covid Tracing Tracker es una base de datos global y dinámica con la finalidad de rastrear la avalancha de aplicaciones que se encargan del rastreo de contactos, y de esta manera, identificar y notificar a todos aquellos que entran en contacto con un operador, creando contactos contagiados por coronavirus de forma automática.

La herramienta informa de cualidades como, su nivel de privacidad, su transparencia y la tecnología base que utiliza el modelo de cada país. Algunas son muy básicas y temporales, mientras que otras son omnipresentes e invasivas; el sistema de China, por ejemplo, reúne datos que incluyen la identidad, la ubicación e incluso el historial de pagos on line para que la policía local pueda vigilar a aquellos que rompan las normas de confinamiento.

En su nivel básico, ésta base de datos crea una lista de aplicaciones de rastreo automatizado de contactos respaldada por los gobiernos nacionales. Su funcionamiento depende de dar respuesta a una serie de preguntas y por cada respuesta afirmativa, la aplicación recibe una estrella. Ésta base de datos se va actualizando, a medida que va recibiendo nuevos datos, por lo que supone una buena gestión de las aplicaciones a nivel global ya que desglosa entre otros ámbitos tan controvertidos como el nivel de privacidad que ofrece.

Se adjunta como Anexo I en el trabajo ,un listado de aplicaciones de rastreo del Covid-19 a nivel global y su afectación respecto a la privacidad, transparencia y tecnología, entre otros aspectos.

5.3 Cómo manejan y obtienen los datos éstas aplicaciones

Cuando una aplicación de seguimiento de contactos, entra en contacto con otro dispositivo que ejecuta la misma aplicación, se produce lo que coloquialmente se denomina “apretón de manos” (handshake), y un intercambio de claves. Estas claves, por lo general cambian continuamente y son generadas en función y de manera exclusiva para el dispositivo. Cuando el dispositivo A está frente al dispositivo B, comparten claves en función de un requisito predeterminado de distancia y tiempo, por ejemplo, dentro de los 2 metros durante 15 minutos. El dispositivo retiene las claves o las pasa a un servidor central. Cuando los usuarios confirman que pueden ser positivos para la infección, todas las claves que han generado se agregan a un sistema en la nube. Todos los demás dispositivos recopilarán esta información con determinada frecuencia para observar si hay una coincidencia con las claves que se han recopilado o si, alternativamente, esta coincidencia se procesará en la nube. Si hay una coincidencia, entonces se advierte a esos usuarios que han estado en contacto con otro dispositivo que ahora informa ser positivo, aunque sin saber de qué dispositivo se trata.

Por lo precedente, cabe decir que si el usuario es identificable y todos los datos son almacenados y procesados de manera centralizada, claramente existe un problema de privacidad, sin embargo, si el usuario no es identificable y el sistema central en la nube solo está procesando coincidencias, esto podría ser más eficiente que pedirle al dispositivo local que realice este procesamiento, especialmente, si el dispositivo final tiene recursos limitados, lo que podría ser el caso en algunas zonas del mundo. Este

enfoque, también le da al sistema centralizado la capacidad de identificar posibles falsos positivos, donde algunos usuarios dicen estar infectados, pero en realidad no lo están. El uso de algoritmos complejos para identificar falsos positivos en un enfoque descentralizado es menos realista debido a las limitaciones en cuanto a recursos.

5.4 Radar Covid-19

Radar covid es la aplicación elegida en España como método electrónico de rastreo para avisar a los contactos de las personas contagiadas de su posible situación de riesgo. La prueba piloto de éste método, se llevó a cabo en la isla de la Gomera, entre el 29 y 31 de julio, en la que se han simulado 4 oleadas de rebrotes. Tras esto, el Ejecutivo ofreció a las Autonomías la posibilidad de instaurarla en sus territorios.
La aplicación es válida para teléfonos Android o iOS y se puede descargar desde Google Play Store o Apple App Store. Aunque ya se puede descargar, aún es necesario que las Comunidades Autónomas la implanten en sus sistemas de salud, ya que sino están activados los protocolos de respuesta, no servirá de nada. Actualmente está activa en las islas Canarias y Baleares y se espera que esté operativa en el resto de España a mediados de septiembre.

5.4.1Como funciona Radar Covid

Radar Covid está desarrollada por Indra[31] y bajo el protocolo diseñado en la herramienta diseñada por Google y Apple. Su uso requiere que esté siempre activado

[31] Es una empresa multinacional española que ofrece servicios de consultoría sobre transporte, defensa, energía, telecomunicaciones, servicios financieros; así como servicios al sector público.

el bluetooth. Además es necesario que sea descargada en los dispositivos por lo que su uso es voluntario y no obligatorio. Si nos descargamos la aplicación y nos encontramos durante al menos 15 minutos a una distancia inferior a dos metros, los smartphones intercambiarán unos ficheros alfanuméricos que se guardan en el terminal durante al menos 14 días. En caso de que nos hagamos un test de Covid-19 y demos positivo, nos facilitarán un código nuevo desde el Servicio Público de Salud que debemos introducir en la aplicación. Las personas con las que se haya tenido contacto recibirán la siguiente notificacion alerta: "Has estado cerca de una persona contagiada". De esta forma, se evalúa el tiempo de exposición y la cercanía para calcular el grado de riesgo. Ni la Autoridad Sanitaria, ni Apple o Google reciben ningún tipo de información al respecto. Solo el usuario sabe que ha recibido una alerta de exposición. Si la aplicación no detecta que hayas estado cerca de alguien contagiada, solo te dirá que tu exposición es baja y te dará una serie de consejos como las medidas de seguridad y el distanciamiento social.

5.4.2 Fuente de datos y privacidad de Radar Covid-19

En relación con lo más arriba expuesto, surge la siguiente cuestión ¿De qué forma aparecen éstos códigos alfanuméricos?, Una vez que la persona de positivo tras una prueba de diagnostico de coronavirus (en adelante, PCR), los servicios sanitarios de la comunidad autónoma en la que se ponga en marcha la aplicación facilitará dicho código. *Los "identificadores efímeros Bluetooth" son códigos pseudo-aleatorios con un tamaño de 16 caracteres (16 bytes, o 128 bits), que se generan por tu teléfono móvil cada 10-20 minutos, a partir de la "clave de exposición temporal" diaria. Estos códigos no contienen información personal, que permita identificar al teléfono móvil o al usuario del mismo. Estos "identificadores efímeros Bluetooth" son*

transmitidos por teléfono móvil varias veces por segundo a dispositivos cercanos, accesibles a través de Bluetooth Low Energy, produciendo un intercambio de códigos aleatorios entre dispositivos para que puedan ser almacenados por teléfonos próximos que hayan descargado la aplicación. De igual manera, cada cinco minutos, el teléfono móvil escuchará los identificadores efímeros Bluetooth que son transmitidos por otros teléfonos móviles que tengan la aplicación y los almacenará para calcular si ha existido proximidad con otro usuario contagiado por COVID-19 a lo largo de los últimos 14 días[32].

En cuanto a la privacidad, se trata de una aplicación totalmente descentralizada, es decir, la información se almacena en el dispositivo de cada usuario y no en centros de datos. Cuenta con la garantía de protocolo más usado en Europa y menos invasivo: el DP-3t[33]. No recurre a la geolocalización por GPS o a las antenas de telefonía, por lo tanto los datos no son cedidos al Gobierno. Los datos que maneja la aplicación sobre sus usuarios no permiten su identificación directa.
Concretamente trabaja con la siguiente información:

- Las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth), a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores. Estas claves no guardan relación alguna con la identidad del usuario, y se suben al servidor para que puedan

[32] Gobierno de España (2020), Politica de Privacidad de la Aplicación Radar Covid, España. Radar Covid. Recuperado de: https://radarcovid.covid19.gob.es/terms-of-service/privacy-policy.html.

[33] Rastreo de proximidad descentralizado para preservar la privacidad es un protocolo de código abierto desarrollado en respuesta a la pandemia de coronavirus 2019-2020 para facilitar el rastreo de contactos digitales de los participantes infectados.

ser descargadas por aplicaciones similares en poder de otros usuarios. Con estas claves, mediante un procesamiento que tiene lugar en el teléfono móvil de forma descentralizada, se puede advertir al usuario sobre el riesgo de contagio por haber estado en contacto reciente con una persona que ha sido diagnosticada por Covid-19, sin que la aplicación pueda derivar su identidad o el lugar donde tuvo lugar el contacto.

- Un código de confirmación de un solo uso de 12 dígitos facilitado por las autoridades sanitarias en caso de prueba positiva por Covid-19. Este código debe ser informado por el usuario para permitir la carga voluntaria de las claves de exposición al servidor.

- Cuestionario voluntario para la recogida de información sobre la experiencia de uso de la aplicación, comprensión de la misma o percepción sobre la privacidad entre otros.

Por lo precedente, cabe decir, que para obtener un resultado óptimo se considera que sobre un 60% de la población debe descargarse ésta aplicación.

5.4.3 Protección y legitimación de los datos utilizados

Dado que radar covid no almacena datos personales, no son de aplicación los derechos de acceso, rectificación, supresión, limitación, oposición y portabilidad, así como, a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos. En caso de reclamaciones o quejas, los usuarios deben presentarlas ante la Agencia Española de Protección de Datos.

La protección de datos no es aplicable en éste caso ya que la aplicación no almacena datos de sus usuarios, en todo caso, las medidas de seguridad implantadas se corresponden con las previstas en el anexo II, (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Así mismo, informan de que tanto el almacenamiento como el resto de las actividades del tratamiento de datos no personales utilizados, estarán siempre ubicados dentro de la Unión Europea.

En cuanto a la legitimación de la información, será de aplicación las siguientes bases legales:

- *El consentimiento del usuario libre, específico, informado e inequívoco del usuario, poniendo a su disposición la presente política de privacidad, que deberá aceptar mediante el marcado de la casilla dispuesta al efecto.*
- *Razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, artículo 9.2 i del Reglamento UE 679/2016, General de Protección de Datos (en adelante, RGPD), para el tratamiento de los datos de salud (por ejemplo, el estado de una persona contagiada o información sobre síntomas, etc.).*
- *Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1 e) RGPD).*

- *Fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos (artículo 9.2 j) RGPD)*[34].

5.5 Programa Datalai en tenerife

Ésta herramienta genera información en tiempo real con datos de viajeros del transporte público que ya tiene el Cabildo de Tenerife por medio de sus empresas Titsa y Metrotenerife, y que se cruzará con la información del Servicio Canario de Salud para hacer un seguimiento de los itinerarios seguidos por personas que hayan resultado positivas a Covid-19. Además, están inmersas en el proyecto otras empresas e instituciones como, el Instituto Tecnológico y de Energías Renovables (ITER), y el Servicio canario de la Salud, la Universidad de La Laguna (ULL), a través del Instituto de Enfermedades Tropicales y Salud Pública y de la Cátedra Cajasiete Big Data, Open Data y Blockchain, el Hospital Universitario Nuestra Señora de la Candelaria y Cajasiete.

El Cabildo de Tenerife, pondrá a disposición del Gobierno de Canarias, los datos obtenidos a través de la telefonía móvil y que desde hace tiempo tiene el área para tomar decisiones acerca de la frecuencia y las líneas de transporte público. Así mismo, se cuenta con datos específicos del periodo de desescalada recopilados recientemente. También pone a disposición de esta iniciativa un equipo de trabajo multidisciplinar y su infraestructura de cómputo y almacenamiento en el

[34] Gobierno de España (2020), Politica de Privacidad de la Aplicación Radar Covid, España. Radar Covid. Recuperado de https://radarcovid.covid19.gob.es/terms-of-service/privacy-policy.html.

superordenador TEIDE HPC[35], tanto para albergar los datos de toda la Comunidad Autónoma de Canarias, como para su procesamiento a través de los modelos basados en inteligencia artificial que se lleven a cabo.

La idea central de éste movimiento de datos reside en asegurar el perímetro recorrido en éstos transportes, de los positivos en Covid 19 durante el estado de emergencia sanitaira, facilitándo y asegurando el trabajo de los rastreadores conociendo los sectores afectados y detectando zonas y población de riesgo. De ésta forma se podrán tomar medidas de control y prevención en determinadas zonas.

Aunque el Cabildo de Tenerife asegura en todo momento el anonimato de los usuarios y el cumplimiento con las leyes de protección de datos, a lo expuesto, no han faltado puntos de vista críticos asegurando que éste proyecto no cumple con leyes que lo legitimen requeridas y lo tildan de invadir la privacidad de sus usuarios, poniendo en tela de juicio el respeto a los derechos fundamentales de los ciudadanos. Existen ciertas discrepancia en cuanto al anonimato de la aplicación, concretamente, el partido político "Sí Podemos" ha argumentado que Datalai incide sobre el derecho fundamental a la intimidad recogido en el art. 18 de la CE, y cuestiona su metodología, alegando la inexistencia de una publicación con la actividad de tratamiento de los datos personales, tal y como se indica en el RGPD.

[35] El supercomputador Teide-HPC se encuentra en el Centro de datos de D-ALiX de la localidad de Granadilla de Abona en la isla de Tenerife. Teide-HPC es el segundo superordenador más potente de España tras el supercomputador MareNostrum. Así mismo, ofrece a investigadores, empresas del Parque Tecnológico y Científico de Tenerife, y a la Universidad de La Laguna, un medio de alta capacidad de proceso, para mejorar y ampliar el alcance tanto nacional como internacional de las investigaciones.

6. Conclusiones

Después de estudiar la utilización de dispositivos o medios técnicos de seguimiento y localización tras la reforma de la LECrim, podemos formular las siguientes conclusiones.

La LO 13/2015, de 5 de octubre, ha supuesto un avance necesario puesto que ha reforzado las garantías procesales, evitando la posible vulneración de derechos fundamentales. Antes de la reforma de la LECrim, ésta no contemplaba una regulación exhaustiva de las numerosas medidas de investigación que han ido surgiendo con el avance de las nuevas tecnologías, lo que repercutía de forma negativa en la investigación y represión de las nuevas formas de criminalidad.

La medida de investigación objeto de estudio en este trabajo carecía de regulación especifica, era una medida elaborada a través de jurisprudencia del TS como una diligencia de investigación legitima desde el punto de vista constitucional. Se utilizaba por las Fuerzas y Cuerpos de Seguridad del Estado en sus investigaciones, sin ningún tipo de restricción judicial, ya que no existía legislación aplicable al respecto y la jurisprudencia la avalaba, puesto que no suponía una violación de derechos fundamentales.

Aunque sin regulación especifica, los Agentes realizaban estas prácticas al amparo de los arts. 282 y 769 de la LECrim, que hacen referencia a las actuaciones de la Policia Judicial, estableciendo como objeto primordial la función de averiguación de los delitos y la práctica de las diligencias necesarias para descubrir a los delincuentes, de igual forma, se pronuncia el art. 11 de la Ley Orgánica de Fuerzas y Cuerpos de Seguridad.

Es decir, los dispositivos de geolocalización (balizas policiales), que permiten

conocer en todo momento la ubicación del sujeto en tiempo y lugar, eran utilizados por las Fuerzas y Cuerpos de Seguridad del Estado avalado por la jurisprudencia del TS.

Sin embargo, como se puede observar a lo largo del trabajo, esta nueva regulación no está carente de problemas que han ido surgiendo en su práctica diaria. La jurisprudencia, en la interpretación de la ley, unifica la doctrina existente al respecto, supliendo ciertas carencias que se observan en la reforma y estableciendo una serie de pautas para su correcta aplicación.

Ahora, la LECrim, exige para la aplicación de esta medida de investigación que las autoridades soliciten con anterioridad a la practica de la medida, la autorización judicial a fin de que sea ésta quien considere la procedencia de la practica de la medida. Sólo en situaciones urgentes la policía podrá adoptar esta medida de oficio, de igual forma, siempre deberán comunicar al Juzgado competente la situación planteada y los términos en los que se ha adoptado la medida, a la mayor brevedad posible, y en todo caso, en el plazo máximo de veinticuatro horas, de esta manera la autoridad judicial podrá ratificar la medida adoptada o acordar su inmediato cese, en el mismo plazo. Por tanto, únicamente será posible la adopción de la medida si el Juez de Instrucción considera que es pertinente y se adecua a las necesidad de la situación concreta.

Lo expuesto, nos lleva a afirmar, que si con anterioridad a la aplicación de esta medida no se cuenta con la debida autorización judicial o no se cumplen los estrictos términos señalados por el Juez Instructor en la autorización judicial, los datos obtenidos en la investigación judicial serán declarados nulos.

Estas diligencias de investigación, solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el

interés público y de terceros. De esta manera, a partir del 6 de octubre de 2015, la solicitud de geolocalización de un objeto vinculado directa o indirectamente a una persona, un vehículo, un velero, exige preceptivamente autorización judicial, pudiendo incurrir en caso contrario la autoridad, funcionario público o agente de ésta, en responsabilidad penal.

Como ya se ha indicado, el uso de geolocalizadores hasta antes de la reforma de la LECrim, era considerado como una herramienta propia de la actividad investigadora de la autoridad, tras la reforma, y con la nueva regulación, entiendo que se obstaculiza la labor policial, ya que aumentan los trámites burocráticos para adoptarla y por tanto, se ralentiza los términos de la investigación pudiendo ocasionar la perdida de evidencias.

Así mismo, entiendo que la injerencia de la geolocalización en el derecho a la intimidad de las personas, es de muy baja intensidad respecto a otras medidas de investigación, ya que un dispositivo de localización da la ubicación de un vehículo, barco, pero no de la persona, incluso con la posibilidad de que la persona que conduzca el vehículo no sea el sujeto investigado.

Curiosamente, la utilización de este tipo de dispositivos de seguimiento y localización en la investigación privada, realizada por los Detectives Privados, no constituye, per se, ninguna conducta ilícita de las tipificadas en el Código Penal, aunque si puede generar vulneraciones en el ámbito civil o laboral, si su uso es desmedido y no siguen razonables criterios de proporcionalidad, necesidad e idoniedad. En esta línea, hay numerosos pronunciamientos judiciales. Las Audiencias Provinciales han creado jurisprudencia, absolviendo a la mayoría de investigadores privados que han sido condenados por este tipo de prácticas, de esta manera, permiten que los mismo utilicen estos dispositivos. El criterio seguido por

varias sentencias en cuanto a la permisión de la utilización de dispositivos GPS por parte de los detectives privados en el ejercicio de su oficio requiere que el trabajo se desarrolle en la vía pública, no restrinja la libertad deambulatoria y la herramienta no sustituya la labor del profesional.

Sin embargo hay que reconocer que existe un vacío legal en este aspecto, ya que el Código Penal castiga a las personas que se apoderen de cartas, papeles, mensajes de correo electrónico o documentos personales ajenos, o bien, a los que pinchen teléfonos; esta medida de investigación protege la intimidad de los ciudadanos. Los juzgadores no niegan que el hecho de que se le coloque a una persona un dispositivo GPS en su vehículo y de esta manera, conocer en tiempo real su ubicación, sea una intromisión en su intimidad, pero no todos los ataques contra la intimidad son constitutivos de delito. El legislador no se ha pronunciado al respecto.

Del mismo modo, de la mano del Covid-19 se han creado aplicaciones móviles que permiten el seguimiento y localización de los ciudadanos, con el fin de controlar la pandemia. Como se ha estudiado en el presente trabajo, el grado de invasión de la aplicación dependerá de numerosas causas, tanto del país en el que se resida, teniendo en cuenta su nivel de democratización y la protección de los derechos fundamentales, como en el uso de la tecnología que se utilice para realizar el seguimiento (Bluetooth o GPS). El procesamiento de los datos personales en estas aplicaciones, plantea relevantes cuestiones que afectan a los derechos fundamentales, como el derecho a la intimidad, ya que infiere en las libertades de los ciudadanos y, concretamente, en lo que se refiere a privacidad y protección de datos.

Un informe de la agencia de los derechos fundamentales de la Unión Europea con sede en Viena, alerta de que, más allá de la vulneración de la privacidad, estas aplicaciones pueden afectar al derecho de libre movimiento, de asociación e incluso de religión, ya que identificar las relaciones de una persona con otros individuos o

sitios, podría revelar creencias religiosas o políticas. Dando respuesta a lo expuesto, cabe decir, que en circunstancias excepcionales se pueden limitar los derechos pero nunca se deben descuidar los principios de necesidad, proporcionalidad y, en todo caso, evitar la discriminación.

En esta línea, la Comisión Europea, ha indicado una serie de criterios que estas aplicaciones deben cumplir, como que su uso sea voluntario, que sean eficaces, que se basen en códigos abiertos, no usen geolocalización**,** empleen los datos de forma anónima y los eliminen una vez extinga la pandemia. Incluso, también hace referencia a otras tecnologías que se usan contra el coronavirus y que causan preocupación, así, el uso de drones para medir la distancia entre personas en espacios públicos y cámaras de control de la temperatura en la calle o en los lugares de trabajo.

Vivimos en la sociedad de la información y la tecnología, donde, cada día, la línea que separa la privacidad y las estrategias de control es, cada vez, más delgada.

Bibliografía

Obras generales, monografías y publicaciones en revistas

BUENO MATA, F,. (2015). Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Recuperado el 11 de abril de 2016, disponible /dialnet.unirioja.es/servlet/articulo.

DÍEZ RIPOLLÉS, J. L. (24 de abril de 2013). Código Procesal Penal. Recuperado 24 de marzo, 2016, de www.juecesdemocracia.es.

GONZÁLEZ-CUÉLLAR SERRANO, N. y MARCHENA GÓMEZ, M., La Reforma de la Ley de Enjuiciamiento Criminal en 2015, Madrid, Castillo de Luna, 2015, p. 173.

GONZÁLEZ-MONTES SÁNCHEZ, J.L., "Reflexiones sobre el Proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas", en Revista Electrónica de Ciencia Penal y Criminología, núm. 17- 06, 2015, p. 21.

JIMÉNEZ SEGADO, C. y PUCHOL AIGUABELLA, M., "Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección de datos", en Diario La Ley, núm. 8676, 2016, p. 2.

LÓPEZ CAUSAPÉ, E., "Las medidas de investigación tecnológica en la ley de enjuiciamiento criminal", Boletín Digital Penal, Asociación Judicial Francisco de Vitoria, julio, 2016.

LÓPEZ GUERRA, L,. (1994). Introducción al Derecho Constitucional. Barcelona: Tirant lo Blanch. págs 23-40.

RAYÓN BALLESTEROS, M. C., "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015", en Anuario Jurídico y Económico Escurialense, LII (2019) 179-204 / ISSN: 1133-3677.

Legislación

Constitución Española, de 27 de diciembre de 1978.

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950.

Ley Orgánica 10/95, de 23 de noviembre, del Código Penal.

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

BOE núm. 239, de 6 de octubre de 2015, páginas 90192 a 90219 [BOE-A-2015-10725].

Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado (FGE), sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización. - BOE, 22-03-2019.

Fuentes de internet

Gobierno de España (2020), Politica de Privacidad de la Aplicación Radar Covid, España. Radar Covid. Recuperado de https://radarcovid.covid19.gob.es/terms-of-service/privacy-policy.html

El Derecho.com (2020), LEFEBVRE, España. El análisis de la colocación de un dispositivo GPS en el vehículo de un investigado. Recuperado en https://elderecho.com/analisis-la-colocacion-dispositivo-GPS-vehiculo-investigado-nuestra-seccion-jurisprudenciatuitatuit

Iberley (2019), España. Utilización de dispositivos tecnicos de seguimiento y localización. Recuperado en :https://www.iberley.es/temas/utilizacion-dispositivos-medios-tecnicos-seguimiento-localizacion-proceso-penal-63153

Welivesecurity (2020), Eset. Apps de rastreo de contactos de COVID-19. Recuperado en https://www.welivesecurity.com/la-es/2020/07/01/apps-rastreo-contactos-covid-19-preocupacion-privacidad/

Averum Abogados (2020), España. Como es el impacto de las apps de rastreo Covid-19 en la proteccion de la intimidad. Recuperado en: https://www.averum.es/actualidad/como-es-el-impacto-de-las-apps-de-rastreo-covid-19-en-la-proteccion-de-la-intimidad

Economist&Jurist (2020). APPs para rastreo del COVID-19 y derecho a la intimidad.Recuperado en: https://www.economistjurist.es/articulos-juridicos destacados/derecho-civil/apps-para-rastreo-del-covid-19-y-derecho-a-la-intimidad/

La Provincia (2020), España. DATALAI: el proyecto piloto que se instalará en Canarias para rastrear el coronavirus. Recuperado en :https://www.laprovincia.es/canarias/2020/05/21/datalai-proyecto-piloto-instalara-*canarias/1284529.html*

ANEXO I

Listado de 'apps' de rastreo de COVID-19

Ubicación	Nombre	Explicación	Voluntario	Limitaciones	Borrado de datos	Datos mínimos	Transparencia	Tecnología
Australia	COVIDSafe	La aplicación de Australia tuvo una implementación rápida al inicio, pero no es compatible con iPhone	★	★	★	★	★	Bluetooth
Austria	COVIDSafe	Austria fue uno de los primeros grandes países europeos en contar con la API de Google/Apple	★	★	★	★	★	Bluetooth, Google / Apple
Bulgaria	ViruSafe	Bulgaria empezó a levantar las restricciones de movimiento a principios de mayo	★	☆	☆	☆	☆	Ubicación
China	Chinese health code system	Hay muy poca información disponible para el público sobre cómo funciona la tecnología de China	☆	☆	☆	☆	☆	Ubicación/ Big Data
Chipre	CovTracer	Implementada en febrero, la aplicación chipriota fue uno de los primeros esfuerzos de lanzamiento	★	☆	☆	★	★	Ubicación
República Checa	eRouska	eRouska es una parte del más amplio plan de "cuarentena inteligente" del Gobierno checo	★	★	★	★	★	Bluetooth
Finlandia	Ketju*	eRouska es una parte del más amplio plan de "cuarentena inteligente" del	★	☆	☆	★	★	Bluetooth, DP-3T
Francia	StopCovid*	Al igual que Reino Unido y Noruega, Francia negoció con Apple y Google, pero decidió no usar sus estándares	★	☆	☆	☆	☆	Bluetooth
Alemania	Corona App*	Alemania optó por la API de Google/Apple después de querer primero construir un sistema centralizado	★	☆	☆	★	☆	Bluetooth, Google/Apple
Ghana	GH COVID-19 Tracker	La aplicación de Ghana se centra en la recogida de datos de ubicación de los usuarios	★	☆	☆	☆	☆	Ubicación
India	Aarogya Setu	India es el único país democrático cuya aplicación es obligatoria para millones de personas	☆	☆	★	★	☆	Bluetooth, Ubicación

Irán	Mask.ir	La original aplicación AC19 covid de Irán fue prohibida por Google Play por recoger más datos de los permitidos	★	☆	☆	☆	☆	Ubicación
Irlanda	Aplicación HSE Covid-19*	A diferencia del vecino Reino Unido, Irlanda optó por utilizar la API de Google/Apple	★	☆	☆	☆	☆	Bluetooth, Google/Apple
Israel	HaMagen	Las autoridades aseguraron que la aplicación no era lo suficientemente precisa porque se basaba solo en GPS e información voluntaria.	★	★	★	★	★	Ubicación
Italia	Immuni*	Después de China, Italia fue el primer país occidental devastado por COVID-19	★	★	☆	★	★	Bluetooth, Google/Apple
Países Bajos	Private Tracer*	Ha habido un debate muy intenso en los Países Bajos sobre la privacidad y la eficacia de las aplicaciones	★	☆	☆	★	★	Bluetooth, DP-3T, Google /Apple
Noruega	Smittestopp	Noruega no adoptó la API de Google/Apple, otro ejemplo de la división europea	★	★	★	★	★	Bluetooth, Ubicación
Polonia	ProteGO*	ProteGO sigue el modelo de los esfuerzos de Singapur.	★	☆	★	★	★	Bluetooth
Singapur	Trace Together	TraceTogether fue la primera gran aplicación de rastreo de contactos vía Bluetooth	★	★	★	★	★	Bluetooth, BlueTrace
Suiza	Swiss Contact Tracing*	Al principio, los suizos decidieron utilizar DP-3T en vez de la API de Google/Apple	★	★	★	★	☆	Bluetooth, DP-3T, Google /Apple
Turquía	Hayat Eve Sığar,	Turquía obliga a las personas que den positivo a descargar la aplicación y luego compartir datos con la policía	☆	☆	☆	★	☆	Bluetooth, Ubicación
Reino Unido	Aplicación NHS COVID-19*	Reino Unido ha sido noticia por su rechazo a implementar la API de Google/Apple	★	☆	☆	★	★	Bluetooth