N/REF: 0113/2019

La consulta plantea si es conforme al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), el tratamiento de datos personales derivado de un sistema de alerta temprana (SAT) realizado a través del envío masivo de mensajes a la población que se encuentre en el archipiélago canario en caso de riesgos que puedan producir situaciones de emergencia.

El SAT se pondría en marcha por el Centro Coordinador de Emergencias y Seguridad (CECOES112), a través de la entidad GESTIÓN DE SERVICIOS PARA LA SALUD Y LA SEGURIDAD EN CANARIAS, S.A., como empresa prestadora del 1-1-2 CECOES en las Islas Canarias, en nombre de la Dirección General de Seguridad y Emergencias de Canarias, organismo público del Gobierno de Canarias responsable de la seguridad y las emergencias en las islas, dependiente de la Consejería de Política Territorial, Sostenibilidad y Seguridad

Para la utilización SAT de envíos masivos de mensajes a teléfonos fijos y a teléfonos móviles, manifiesta la consultante que utilizarían la información de los destinatarios obtenida principalmente de tres fuentes:

(i) la base de datos de números de teléfonos de llamantes al 112 obtenida a partir de la base de datos que facilita la CNMC

(ii) los datos de los usuarios que se hayan dado de alta en la App del 112

(iii) la base de datos facilitada por la CNMC, (en este supuesto en la consulta no se especifica si las personas incluidas han llamado previamente al 112, por lo que debido a la determinación del primer supuesto, se sebe entender que no han llamado al 112).

Asimismo distingue si la llamada se realiza desde un **teléfono fijo** la localización se obtiene a partir de los datos que obran en la base de datos facilitada por la CNMC para identificar las llamadas de emergencia recibida en el servicio 112 y si la llamada se realiza desde un **teléfono móvil**, manifiestan que "*la localización se obtiene en base a las antenas móviles (esta información nos la aportan los proveedores de telefonía móvil en el momento de la comunicación ciudadano - servicios de emergencia), y posteriormente se refleja por cada llamada realizada al 1-1-2 un incidente con una localización o dirección facilitada por el alertante. Para cada llamada recibida en el 112, se almacena su posicionamiento en la base de datos del CTPhone, en la tabla callparameters*"

I

Con carácter previo al análisis de las implicaciones jurídico-normativas del SAT, debe concretarse los elementos fácticos del sistema para ofrecer una respuesta conforme a derecho.

Del supuesto de hecho de la consulta se deduce que se pretende enviar mensajes SMS/MMS para líneas de teléfono móviles, o locuciones de voz para el caso de líneas de teléfono fijo, **basado en la ubicación de los dispositivos** en la medida en que se encuentren en una localización dónde se hayan producido (…)*situaciones de grave riesgo, catástrofe o calamidad pública de las situaciones que se desglosan en el PLATECA aprobado por el Gobierno de Canarias*,(…) que se aporta a la consulta y que bajo la clasificación de Riesgos Naturales, Riesgos Antrópicos, Riesgos Tecnológicos se identifican hasta 45 acontecimientos, que van desde, movimientos sísmicos o plagas de langosta, hasta accidentes en el mar, pasando por acontecimientos deportivos como rallies.

Por tanto, deben diferenciarse a los efectos de resolver la consulta planteada, tres categorías de destinatarios de la información, o dicho de otro modo, tres posibles fuentes de obtención de los datos, teniendo en cuenta la finalidad del SAT, que según consta en la consulta sería (…)*reducir los daños infligidos por los peligros en las personas que puedan resultar afectadas o se encuentren el ámbito territorial de afectación.(…)*

Para determinar la localización de los afectados, se indica que para los **teléfonos fijos** se utilizaría la información que consta en la base de datos proporcionada por la CNMC (hayan llamado o no al 112), para **teléfonos móviles**, la información sobre las antenas de telefonía que aportan los operadores de telecomunicaciones cuando realicen una llamada al 112 y la propia información que el llamante haya proporcionado durante la llamada. Y una tercera opción es la información que proporcione la **aplicación de emergencias** para dispositivos móviles respecto de aquellos usuarios que la hayan instalado.

En definitiva, a los efectos de cumplir la finalidad del SAT se deduce que se pretende crear o disponer de una base de datos de líneas de teléfono (fijos y/o móviles) que estén geolocalizados y en caso de producirse una de las 45 situaciones de emergencia previstas en el PLATECA dónde estos se encuentren, realizar los envíos masivos de alerta.

II

Teniendo en cuenta lo anterior, del actual marco normativo en materia de protección de datos, debemos destacar el artículo 5 del RGPD que recoge los principios relativos al tratamiento, a cuyo tenor los datos personales serán:

> *a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);*

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; (…) («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

III

De los principios indicados y en relación con el objeto de la consulta, debe ponerse especial atención en los de **licitud y transparencia**, **limitación de finalidad** y **limitación del plazo de conservación.**

En cuanto al *principio de licitud*, el artículo 6.1 del RGPD dispone lo siguiente:

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

La consultante propone como posibles bases jurídicas del tratamiento, en primer lugar, las previstas en el apartado c) y en el apartado e) del artículo 6.1 del RGPD y en último término la prevista en el apartado d) relativa a la necesidad de proteger intereses vitales del interesado o de otra persona física.

En relación a las primeras, el artículo 8 de la LOPDGDD, bajo la rúbrica *Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos*. dispone lo siguiente:

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

De acuerdo con lo expuesto, procede analizar el régimen jurídico aplicables a los servicios de emergencia y protección civil en general, y al CECOES 112 de Canarias en particular, teniendo en cuenta a su vez el origen de los datos que se pretende someter a tratamiento con la implantación del SAT.

En cuanto a la normativa de ámbito estatal, procede acudir a la **Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil**,(Ley de Protección Civil en lo sucesivo) establece lo siguiente:

Artículo 1.1 *La protección civil, como instrumento de la política de seguridad pública, es el servicio público que protege a las personas y bienes garantizando una respuesta adecuada ante los distintos tipos de emergencias y catástrofes originadas por causas naturales o derivadas de la acción humana, sea ésta accidental o intencionada.*

Artículo 3. El Sistema Nacional de Protección Civil

1. El Sistema Nacional de Protección Civil integra la actividad de protección civil de todas las Administraciones Públicas, en el ámbito de sus competencias, con el fin de garantizar una respuesta coordinada y eficiente mediante las siguientes actuaciones:

a) Prever los riesgos colectivos mediante acciones dirigidas a conocerlos anticipadamente y evitar que se produzcan o, en su caso, reducir los daños que de ellos puedan derivarse.(…)

Artículo 6. Derecho a la información

1 *Todos tienen derecho a ser informados adecuadamente por los poderes públicos acerca de los riesgos colectivos importantes que les afecten, las medidas previstas y adoptadas para hacerles frente y las conductas que deban seguir para prevenirlos.*

2.Dichas informaciones habrán de proporcionarse tanto en caso de emergencia como preventivamente, antes de que las situaciones de peligro lleguen a estar presentes.

Artículo 7 bis Deber de colaboración

1. Los ciudadanos y las personas jurídicas están sujetos al deber de colaborar, personal o materialmente, en la protección civil, en caso de requerimiento de la autoridad competente de acuerdo con lo establecido en el artículo 30.4 de la Constitución y en los términos de esta ley.(…)

5. Las medidas restrictivas de derechos que sean adoptadas o las que impongan prestaciones personales o materiales tendrán una vigencia limitada al tiempo estrictamente necesario para hacer frente a las emergencias y deberán ser adecuadas a la entidad de la misma.(…)

8. Los medios de comunicación están obligados a colaborar de manera gratuita con las autoridades en la difusión de las informaciones preventivas y operativas ante los riesgos y emergencias en la forma que aquéllas les indiquen y en los términos que se establezcan en los correspondientes planes de protección civil.

Por su parte, el **Real Decreto 903/1997, de 16 de junio, por el que se regula el acceso, mediante redes de telecomunicaciones, al servicio de atención de llamadas de urgencia a través del número telefónico**, establece lo siguiente:

Artículo 2 Acceso al número 112

1. El número telefónico 112 podrá utilizarse por los ciudadanos para requerir, en casos de urgente necesidad, la asistencia de los servicios públicos competentes en materia de atención de urgencias sanitarias, de extinción de incendios y salvamento, de seguridad ciudadana y, por la posible necesidad de coordinar los anteriores, de protección civil, cualquiera que sea la Administración pública de la que dependan.

2. Para garantizar la respuesta y atención adecuadas de las llamadas que se produzcan y asegurar una actuación rápida, ordenada y eficaz de los mencionados servicios, en el ámbito de las funciones y competencias que a cada uno le correspondan, las entidades prestatarias del servicio de atención de llamadas de urgencia 112 adoptarán las medidas necesarias en relación con los servicios de urgencia de su dependencia y establecerán los acuerdos o convenios de colaboración que sean precisos cuando tales servicios no sean de su titularidad.

Artículo 3 Condiciones de acceso al servicio de atención de llamadas de urgencia

3.(…)*dichos operadores facilitarán la identificación automática de la línea o zona geográfica desde donde se efectúen las llamadas al número telefónico 112, dentro de las posibilidades técnicas de la red y de acuerdo con la regulación que sobre las facilidades de presentación y limitación de la línea llamante se establezcan en la normativa nacional y comunitaria para salvaguardar la seguridad nacional, la defensa, la seguridad pública y la prevención, investigación y persecución de delitos, la seguridad de la vida humana o razones de interés público.*

En todo caso, lo establecido en el párrafo anterior se entenderá sin perjuicio de las medidas que se adopten para garantizar el secreto de las comunicaciones, de acuerdo con lo establecido en el artículo 18.3 de la Constitución, y la protección de los datos personales, conforme a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y en sus normas de desarrollo y disposiciones complementarias.

Artículo 5 De la prestación del servicio de atención de llamadas de urgencia 112

1. La prestación del servicio de atención de llamadas de urgencia 112 se llevará a cabo por las Comunidades Autónomas que establecerán los correspondientes centros de recepción de llamadas de urgencia y las redes que, en su caso, fuera necesario instalar para establecer otros puntos de atención de los servicios públicos que hubieran de proporcionar la asistencia objeto de las llamadas de urgencia.

En cuanto a la normativa autonómica, procede citar en primer lugar la **Ley 9/2007, de 13 de abril, del Sistema Canario de Seguridad y Emergencias,** que dispone lo siguiente:

Artículo 4 Derechos de los ciudadanos en materia de seguridad y emergencias

> *a) A tener garantizada la confidencialidad de sus actuaciones privadas en las que pudiera verse comprometido en relación a la seguridad.*
>
> *b) A la intimidad*.(…)
>
> *d) A una información pública veraz, detallada y periódica acerca de los riesgos de agresión delictiva, accidente o calamidad pública a la que se vean expuestas las personas*.(…)
>
> *2. Los ciudadanos tienen el derecho a recibir información relativa a los riesgos que puedan afectarle, las consecuencias de los mismos que sean previsibles y las medidas de autoprotección y conductas a seguir, en el marco de lo dispuesto en los planes de emergencia.*

Artículo 37 Información

> *En caso de emergencia, las Administraciones Públicas canarias con competencias en materia de protección civil velarán porque existan los mecanismos adecuados para transmitir a la población los avisos, comunicados e instrucciones de autoprotección. A estos efectos recabarán la colaboración de los medios de comunicación social.*

En segundo lugar, **Decreto 62/1997, de 30 de abril, por el que se regula la implantación del Servicio de Atención de Urgencias y Emergencias a través del Teléfono Único Europeo de Urgencias 112**, dispone lo siguiente:

> *(…)Este nuevo servicio al público podrá utilizarse por los ciudadanos para requerir, en casos de urgente necesidad, la asistencia de los servicios públicos y competentes en materias de atención de urgencias y emergencias sanitarias, de extinción de incendios y salvamento, de seguridad ciudadana y de protección civil, cualquiera que sea la Administración pública de la que dependan.(…)*

Artículo 2.- Definición del servicio.

> *1. Este servicio podrá utilizarse, en el ámbito territorial de la Comunidad Autónoma de Canarias, para requerir, en casos de urgente necesidad, la asistencia de los servicios competentes en materias de atención de emergencias y urgencias sanitarias, de extinción de incendios y salvamento, de seguridad ciudadana y de protección civil, cualquiera que sea la Administración pública de la que dependan.*

Artículo 3.- Órganos competentes.

> *Los órganos competentes de la Comunidad Autónoma de Canarias para ejercer las facultades a que se refiere el presente Decreto serán los que*

tengan atribuidas las competencias en materia de seguridad, sin perjuicio de los que puedan corresponder a otros órganos.

En tercero lugar, el **Decreto 137/2016, de 24 de octubre, por el que se aprueba el Reglamento Orgánico de la Consejería de Política Territorial, Sostenibilidad y Seguridad**, dispone en el Capítulo VIII referido a la Dirección General de Seguridad y Emergencias, lo siguiente:

Artículo 46 Funciones generales en materia de seguridad, emergencias y protección civil

2. La coordinación en materia de protección civil, así como la planificación, dirección, coordinación y control del Servicio de Atención de Urgencias y Emergencias creado por el Decreto 62/1997, de 30 de abril, y de los distintos servicios en materia de seguridad y emergencias. (…)

7. Promover y coordinar la actuación operativa de los diferentes recursos actuantes en la atención y respuesta a incidentes y accidentes en los que intervengan diferentes sectores de seguridad y emergencias. (…)

Artículo 49 Funciones específicas en materia de emergencias, protección civil y salvamento marítimo(…)

10. Bajo las directrices del Consejero o Consejera, ejercer la tutela funcional y coordinación del Centro Coordinador de Emergencias y Seguridad (CECOES), lo que no comportará relación laboral alguna con los trabajadores del mismo.

Disposición adicional quinta Centro Coordinador de Emergencias y Seguridad

Se establece como Centro Coordinador de Emergencias y Seguridad del Gobierno de Canarias (CECOES) el Centro 1-1-2 del Servicio de Atención de Urgencias y Emergencias, creado mediante el Decreto 62/1997, de 30 de abril, el cual actuará como Centro de Coordinación Operativa (CECOP) y Centro de Coordinación Operativa Integrado (CECOPI) previstos en el Plan Territorial de Emergencias de Protección Civil de la Comunidad Autónoma de Canarias (PLATECA).

En cuarto lugar, la **Orden de 21 de diciembre de 1999**, por la que se determina el marco de funcionamiento del Centro Coordinador de Emergencias y Seguridad (CECOES), establece lo siguiente:

Artículo segundo.- Definición y prestación del servicio.

El Centro Coordinador de Emergencias y Seguridad se define como un servicio administrativo que aglutina racionalmente y coordina operativamente las actividades y servicios de las organizaciones de carácter público y privado en que su actividad esté directa o indirectamente relacionada con la prevención, planificación, atención, socorro, seguridad, asistencia técnica o profesional de personas, bienes

o derechos en operaciones de seguridad y emergencia sea cual fuere la naturaleza del hecho que la origine.

Artículo tercero.- Funciones.

El Centro Coordinador de Emergencias y Seguridad (CECOES) es el órgano a través del cual la Administración Pública de la Comunidad Autónoma de Canarias canaliza y coordina las situaciones que afecten al normal desarrollo de la vida cotidiana en materia de seguridad y emergencias. Específicamente se encargará de:

a) Recibir las demandas de auxilio de los ciudadanos y visitantes, a través del Teléfono Único de Urgencia 1-1-2 (uno, uno, dos) u otros que se pudieran establecer con el fin de facilitar información a los ciudadanos y visitantes.

j) Informar a la población y público en general sobre la previsión y actuación en situaciones de emergencia.

Artículo séptimo.- Prestación y dirección del servicio.

El Centro de Coordinación de Emergencias y Seguridad es un servicio al público de la Administración Pública de la Comunidad Autónoma de Canarias prestado en régimen de gestión directa a través de una sociedad pública(…)

Del régimen jurídico expuesto en relación con el tratamiento que propone la consulta se extraen las siguientes conclusiones.

La administración pública consultante, a través de los organismos competentes y departamentos dependientes, puede realizar el tratamiento de datos personales que se derive de la gestión de los servicios de emergencias que les corresponden.

Ahora bien, de las disposiciones estudiadas y en relación con el tratamiento que propone la consultante, se derivan en términos generales, dos actuaciones que pudieran llevar aparejado un tratamiento de datos personales.

La primera es la relativa a la circunstancia de que alguien realice una llamada al 112 para requerir sus servicios y por tanto el CECOES atienda la llamada de emergencia y coordine las actuaciones.

Por lo que tal y como se expondrá a continuación, el uso de la información de aquellas personas que hayan llamado al 112 lo es únicamente a estos efectos, y a partir de ahí, **la base jurídica aplicable a este tratamiento seria la prevista en el artículo 6.1 e) del RGPD en relación con el articulo 8.2 LOPDGDD, y la prevista en el artículo 6.1 d) del RGPD.**

La segunda es aquella que realice la administración consultante, al amparo del **derecho a recibir información** sobre situaciones de riesgo o emergencia del que son titulares los destinatarios de la norma, de acuerdo con el artículo 4 de la Ley 9/2007, de 13 de abril, del Sistema Canario de Seguridad y Emergencias, que también recoge el **derecho a la intimidad** y a **la confidencialidad de sus actuaciones privadas**.

En efecto, entre las funciones que la Orden de 21 de diciembre de 1999, atribuye al Centro Coordinador de Emergencias y Seguridad (CECOES), se encuentra la de *Informar a la población y público en general sobre la previsión y actuación en situaciones de emergencia,* **lo que debe interpretarse a tenor del artículo 37 de la citada ley, en cuanto que para esa función *recabarán la colaboración de los medios de comunicación social,*** y en el mismo sentido la Ley de Protección Civil, en su artículo 7 bis apartado 8 que establece el deber de colaboración a estos efectos de los medios de comunicación social.

No obstante lo anterior, **el ejercicio de competencias y/o la existencia de un interés público no legitima cualquier tipo de tratamiento de datos personales, sino que deberá estarse, en primer lugar, a las condiciones que haya podido establecer el legislador, tal como prevé el propio artículo 6 del RGPD, en sus apartados 2 y 3, así como a los ya citados principios del artículo 5 del RGPD, especialmente a los de limitación de la finalidad y minimización de datos.**

Por consiguiente, el tratamiento que propone la consultante, en relación con los datos de localización de dispositivos móviles aportados por las operadoras y los datos de la dirección administrativa de las líneas de telefonía fija (CNMC) a los fines que obedece el SAT, tal y como veremos, no encuentra amparo en las disposiciones estudiadas.

Por lo que llegados a este punto conviene adelantar ya que la observancia de los **principios de limitación de finalidad, de minimización y de limitación del plazo de conservación** previstos en el artículo 5 del RGPD, hace que de las tres posibles fuentes de datos a utilizar por el SAT, únicamente la relativa a la aplicación de emergencias para dispositivos móviles tenga cabida en el actual marco normativo a los efectos pretendidos por el SAT, previo cumplimiento de determinados requisitos que se analizan en los apartados siguientes.

IV

Respecto del tratamiento de los **datos personales derivado de la utilización del servicio de emergencias 112**, debe tenerse en cuenta que se pretende utilizar tanto la base de datos que proporciona la CNMC, como la información que los operadores de telecomunicaciones dispongan en relación con la geolocalización de las llamadas, a través de las estaciones base (antenas de telecomunicaciones).

Sobre la utilización de la información que proporcionan los operadores de telecomunicaciones en relación con los servicios de telefonía móvil, para la gestión de los servicios de emergencia, debe citarse en primer lugar lo indicado en la **Directiva 2018/1972, del Parlamento Europeo y del Consejo, de 11 de diciembre, por la que se establece el Código Europeo de Comunicaciones Electrónicas** que establece en su **artículo 109.6** que:

Los Estados Miembros velaran por que la información relativa a la ubicación de las personas que efectúan llamadas se ponga a disposición del PSAP más indicado inmediatamente tras el establecimiento de la comunicación de emergencia. Dicha información incluye los datos sobre ubicación de la red y, si están disponibles, los datos relativos a la localización del llamante procedentes del dispositivo móvil. Los Estados miembros garantizarán que el establecimiento y la transmisión de la información relativa a la localización del llamante sea gratuita para este último y para el PSAP con respecto a todas las comunicaciones de emergencia al número único europeo de emergencia «112»

Asimismo en el Considerando 290 se indica que:

"La información sobre la localización del llamante, aplicable a todas las comunicaciones de emergencia, mejora el nivel de protección y seguridad de los usuarios finales y facilita a los servicios de emergencia el ejercicio de sus funciones, siempre que la transferencia a los servicios de emergencia correspondientes de la comunicación de emergencia y de los datos asociados esté garantizada por el sistema nacional de PSAP. La recepción y el uso de esta información sobre la localización del llamante, que incluye tanto la información relativa a la ubicación basada en redes como, cuando se disponga de ella, la información relativa a la ubicación basada en el terminal del llamante, debe ajustarse al Derecho de la Unión aplicable sobre el tratamiento de datos personales y medidas de seguridad. Las empresas que aportan la localización basándose en la red deben poner la información sobre la localización del llamante a disposición de los servicios de emergencia tan pronto como la llamada llegue a ese servicio, independientemente de la tecnología utilizada.

No obstante, las tecnologías de localización basadas en el terminal se han demostrado bastante más exactas y rentables debido a la disponibilidad de datos facilitados por el sistema europeo de navegación por complemento geoestacionario, el sistema de satélite Galileo y otros sistemas mundiales de navegación por satélite y datos wifi. Por lo tanto, la información sobre la localización del llamante obtenida del terminal debe complementar la información de localización basada en la red, incluso en caso de que solo se disponga de ella después de establecida la comunicación de emergencia. Los Estados miembros deben velar por que, siempre que sea posible, la localización del llamante obtenida del terminal se ponga a disposición del PSAP más apropiado.

Lo indicado hasta ahora pone de manifiesto la importancia de la información sobre la localización del llamante a un servicio de emergencias 112 y la obligación de su comunicación a dichos servicios 112 y similares, conocidos como PSAP por sus siglas en inglés.

Asimismo, en el Considerando 294 se indica lo siguiente:

Siempre que se garantice el alcance a todos los usuarios finales afectados independientemente del lugar o del Estado miembro en que residan y se respete el nivel más alto de seguridad de los datos, los Estados miembros deben poder realizar la transmisión de alertas al público mediante servicios de comunicaciones electrónicas disponibles al público distintos de los servicios móviles de comunicaciones interpersonales basados en numeración y de los servicios de transmisión empleados para radiodifusión o por aplicaciones móviles transmitidas a través de servicios de acceso a internet. A fin de informar a los usuarios finales que entren en un Estado miembro de la existencia de tales sistemas de alerta pública, el Estado miembro en cuestión debería garantizar que los usuarios finales reciban automáticamente, por medio de un SMS, sin demoras indebidas y de forma gratuita, información fácilmente comprensible sobre la manera de recibir avisos incluso en equipos terminales móviles no habilitados para servicios de acceso a internet. Las alertas al público distintas de las que dependen de servicios móviles de comunicaciones interpersonales basados en numeración deben transmitirse a los usuarios finales de una manera que resulte fácil de recibir.

Cuando un sistema de alerta al público se base en una aplicación, no se debe exigir a los usuarios finales que se den de alta o se registren ante las autoridades o el proveedor de la aplicación. Los datos de ubicación de los usuarios finales deben usarse conforme a la Directiva 2002/58/CE. La transmisión de alertas al público debe ser gratuita para los usuarios finales. En su revisión de la aplicación de la presente Directiva, la Comisión también podría evaluar si, de conformidad con el Derecho de la Unión, resulta posible y factible crear un único sistema de alerta pública para alertar al público en caso de grandes catástrofes o emergencias inminentes o en curso en varios Estados miembros.

De lo indicado se desprende, en primer término, que los datos de ubicación de los usuarios finales en el caso de ser utilizados en un sistema de alerta pública se realizará conforme a la Directiva 2002/58/CE, y en segundo lugar, que existe la posibilidad de que por parte de los Estados Miembros y con la previa evaluación de la Comisión Europea de que se establezca un sistema de alerta pública de conformidad con el Derecho de la Unión, lo que podría habilitar el tratamiento de los datos utilizados a tal fin, al margen del consentimiento del afectado, siempre y cuando su regulación se encuentre en una norma con rango de ley, respetando el principio de proporcionalidad y con suficientes garantías para que sea conforme al artículo 6.1.e) del RGPD y al artículo el 8.2 LOPDGDD.

En segundo lugar, procede citar el **Informe 39/2019**, dónde se analiza la base jurídica del tratamiento de datos personales derivado del cumplimiento de la obligación de facilitar dicha información, y la comunicación de datos obrantes en la base de datos de la CNMC a los mismos efectos de localizar y atender la llamada recibida en dichos servicios desde un dispositivo fijo. En el citado informe se indica lo siguiente: (…)

II

En primer lugar, la presente consulta se refiere al tratamiento de los datos de localización obtenidos directamente por terminal móvil utilizado, debiendo entenderse por **datos de localización**, conforme al artículo 2 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, (…), "*cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público*"

Tal y como señalaba el Dictamen 5/2005 del Grupo del Artículo 29 sobre el uso de los datos de geolocalización con vista a prestar servicios con valor añadido, en los últimos años se ha producido un aumento espectacular del uso de los datos de localización, debido al "*aumento exponencial en el uso de los datos de localización vía satélite, que en la actualidad pueden ser muy precisos y valiosos, especialmente por lo que se refiere a la asistencia a personas en apuros*" y a "l*a difusión sin precedentes de la telefonía móvil, merced a la cual cada usuario lleva siempre un dispositivo mediante el cual se le puede localizar*".

De ahí que el citado Dictamen destacara que "*dado que el tratamiento de estos datos es un asunto especialmente sensible por referirse a la cuestión esencial de la libre circulación de las personas de forma anónima, el legislador europeo, teniendo en cuenta las consideraciones de las autoridades europeas de protección de datos, ha adoptado normas específicas que establecen la obligación de recabar el consentimiento de los usuarios o abonados antes de proceder al tratamiento de los datos de localización necesarios para prestar un servicio con valor añadido y de informar a los usuarios o abonados de las condiciones de dicho tratamiento* (Artículo 9 de la Directiva 2002/58/CE de 12 de julio de 2002).

Por otro lado, debe atenderse a la definición que de **servicios con valor añadido** efectúa la letra g) de dicha Directiva calificando como tales "*Todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación*"

Dispone el **artículo 9** de la Directiva 2002/58/CE respecto de los **datos de localización** distintos de los datos de tráfico lo siguiente:

"*1. En caso de que puedan tratarse datos de localización, distintos de los datos de tráfico, relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido.*

El proveedor del servicio deberá informar a los usuarios o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio con valor añadido. Se deberá ofrecer a los usuarios y abonados la posibilidad de retirar en todo momento su consentimiento para el tratamiento de los datos de localización distintos de los datos de tráfico.

2. Cuando se haya obtenido el consentimiento de un usuario o abonado para el tratamiento de datos de localización distintos de los datos de tráfico, el usuario o abonado deberá seguir contando con la posibilidad, por un procedimiento sencillo y gratuito, de rechazar temporalmente el tratamiento de tales datos para cada conexión a la red o para cada transmisión de una comunicación.

3. Sólo podrán encargarse del tratamiento de datos de localización distintos de los datos de tráfico de conformidad con los apartados 1 y 2 personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público o del tercero que preste el servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario a efectos de la prestación del servicio con valor añadido."

Consecuentemente, en relación con el tratamiento de los datos de localización para la prestación de servicios de valor añadido, esta Agencia viene invocando la normativa de transposición del citado artículo de la Directiva, constituida en un primer momento por el artículo 38.3 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y, en el momento actual, por el **artículo 48.2.c)** de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, norma especial cuya aplicación prevalece sobre el Reglamento, que dispone que:

"*Respecto a la protección de datos personales y la privacidad en relación con los datos de tráfico y los datos de localización distintos de los datos de tráfico, los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos: c) A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo*

necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado. Los usuarios finales dispondrán del derecho de retirar su consentimiento en cualquier momento y con efecto inmediato para el tratamiento de los datos de localización distintos de tráfico."

Por consiguiente, de acuerdo con lo dispuesto en el **artículo 6.1 a) del RGPD**, la base legal que permite dicho tratamiento será el consentimiento expreso de los usuarios afectados manifestado de manera específica.

No obstante, en el presente caso nos encontramos ante un supuesto diferente, atendiendo a que **no se trataría propiamente de un servicio de valor añadido** y, especialmente, a la finalidad perseguida por el tratamiento, consistente en facilitar la localización del llamante por teléfono móvil a los servicios de emergencia a través de los centros de atención a llamadas de emergencia (servicios 112 y similares) y que es objeto de una regulación específica en nuestro ordenamiento jurídico.

A este respecto, debe recordarse que el **Real Decreto 903/1997, de 16 de junio**, por el que se regula el acceso, mediante redes de telecomunicaciones, al servicio de atención de llamadas de urgencia a través del número telefónico 112 señala, en su **artículo 2.1** que "*El número telefónico 112 podrá utilizarse por los ciudadanos para requerir, en casos de urgente necesidad, la asistencia de los servicios públicos competentes en materia de atención de urgencias sanitarias, de extinción de incendios y salvamento, de seguridad ciudadana y, por la posible necesidad de coordinar los anteriores, de protección civil, cualquiera que sea la Administración pública de la que dependan*", estableciendo en su **artículo 3.3** la obligación de los operadores de redes telefónicas públicas y de servicios de telefonía básica, de redes digitales de servicios integrados y de redes de telefonía móvil automática de facilitar "*la identificación automática de la línea o zona geográfica desde donde se efectúen las llamadas al número telefónico 112, dentro de las posibilidades técnicas de la red y de acuerdo con la regulación que sobre las facilidades de presentación y limitación de la línea llamante se establezcan en la normativa nacional y comunitaria para salvaguardar la seguridad nacional, la defensa, la seguridad pública y la prevención, investigación y persecución de delitos, la seguridad de la vida humana o razones de interés público*".

Añadiendo que "*En todo caso, lo establecido en el párrafo anterior se entenderá sin perjuicio de las medidas que se adopten para garantizar el secreto de las comunicaciones, de acuerdo con lo establecido en el artículo 18.3 de la Constitución, y la protección de los datos personales, conforme a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter*

Personal, y en sus normas de desarrollo y disposiciones complementarias".

Dicha obligación se desarrolla por la **Orden de 14 octubre de 1999** sobre condiciones de suministro de información relevante para la prestación del servicio de atención de llamadas de urgencia a través del número 112, cuyo Preámbulo destaca la importancia de disponer del dato de localización, señalando que "*las entidades prestatarias del servicio de llamadas de urgencia necesitan, para su actuación rápida y eficaz, conocer, en breve espacio de tiempo, no sólo la identificación de la línea llamante, sino también la dirección del titular de la línea telefónica fija o la localización geográfica (servicios móviles) desde la que se ha efectuado la llamada*".

De ahí que su artículo 1 disponga que "*Los operadores del servicio telefónico disponible al público y de redes que den soporte a dicho servicio, a que se refiere el artículo 3 del Real Decreto 903/1997, de 16 de junio, por el que se regula el acceso, mediante redes de telecomunicaciones, al servicio de atención de llamadas de urgencia a través del número telefónico 112, deberán facilitar, dentro de las posibilidades técnicas de las redes, la información de la dirección de la línea desde donde se produce la llamada, en el caso de que ésta se origine en una red fija, incluidas las líneas destinadas a la conexión de terminales de uso público, o de la situación de la celda, es decir, de la zona geográfica en la que se ha recogido la llamada, en el supuesto de que la llamada se origine en líneas de terminación de redes públicas de telefonía móvil. En función de la evolución técnica de estas últimas redes, los operadores facilitarán datos más precisos sobre la ubicación del usuario llamante*".

Y, a los efectos del presente informe, interesa destacar su **artículo 4** "Condiciones para la utilización de la información":

"*La cesión de datos personales referidos en el artículo 2 se entenderá amparada por la protección del interés vital del llamante, la seguridad pública y la protección del interesado o de los derechos y libertades de otras personas y quedará sometida a la legislación de protección de datos, Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal y su normativa de desarrollo. Dicha cesión de datos será utilizada, de manera exclusiva, como soporte para una más efectiva prestación de los servicios de atención de llamadas de urgencia a través del número 112 y será responsabilidad de la entidad prestataria el adecuado uso de los mencionados datos.*

Los datos sobre la ubicación geográfica de las estaciones bases de las redes públicas de telefonía móvil se utilizarán exclusivamente para la prestación del servicio de atención de llamadas de urgencia, no pudiéndose utilizar para otros fines ni cederse a terceros".

Por su parte, la **Ley 9/2014, de 9 de mayo, General de Telecomunicaciones**, señala en su **artículo 28**, relativo a "Otras obligaciones de servicio público", dentro de su apartado 4, que "*los operadores pondrán gratuitamente a disposición de las autoridades receptoras de dichas llamadas (llamadas de emergencia) la información que mediante real decreto se determine relativa a la ubicación de su procedencia.(…)* Y en su **artículo 48,** ya citado anteriormente, sobre el "*Derecho a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas, con los datos de tráfico y de localización y con las guías de abonados*" (…)

Dicho precepto se desarrolla por el **artículo 70** 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 los usuarios**:

"1*. En el caso de que puedan tratarse datos de localización, distintos de los datos de tráfico, relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento expreso de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido.*

A estos efectos, los sujetos obligados deberán dirigirse a los usuarios o abonados, al menos, con un mes de antelación al inicio de la prestación del servicio con valor añadido, e informarles del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a los efectos de la prestación del servicio con valor añadido, y solicitarles su consentimiento para el tratamiento de los datos. Esta comunicación, que deberá efectuarse por un medio que garantice su recepción por el usuario o abonado, podrá llevarse a cabo de forma conjunta a la facturación del servicio prestado por los sujetos obligados al abonado.

Se entenderá que existe consentimiento expreso cuando el usuario o el abonado se dirijan al sujeto obligado y le soliciten la prestación de los servicios con valor añadido que exijan el tratamiento de sus datos de localización.

En todo caso, los usuarios o abonados deberán contar con la posibilidad de retirar en cualquier momento su consentimiento para el tratamiento de sus datos de localización distintos de los de tráfico al que se refiere este apartado, así como de rechazar temporalmente el tratamiento de tales datos, mediante un procedimiento sencillo y gratuito, para cada conexión a la red o para cada transmisión de una comunicación.

2. Cuando se haya obtenido el consentimiento de un usuario o abonado para el tratamiento de datos de localización distintos de los datos de tráfico, el usuario o abonado deberá seguir contando con la posibilidad, por un procedimiento sencillo y gratuito, de rechazar temporalmente el tratamiento de tales datos para cada conexión a la red o para cada transmisión de una comunicación.

3. Sólo podrán encargarse del tratamiento de datos de localización distintos de los datos de tráfico de conformidad con los apartados 1 y 2 las personas que actúen bajo la autoridad del operador de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público o del tercero que preste el servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario a efectos de la prestación del servicio con valor añadido.

4. No obstante lo dispuesto en este artículo, los operadores facilitarán los datos de localización distintos a los datos de tráfico a las entidades autorizadas para la atención de las de urgencia, cuando el destino de las llamadas corresponda a tales entidades".

Por lo tanto, nuestro ordenamiento jurídico establece **la obligación de facilitar a los servicios de emergencia los datos de localización**, amparándose dicha obligación, entre otras circunstancias, **en la necesidad de proteger el interés vital del llamante.**

III

(…)Por tanto, el tratamiento del dato de localización se encontraría amparado en la letra d) del artículo 6.1. del RGPD*: el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física*, independientemente de quién realice dicho tratamiento, ya que en este caso el factor determinante de la licitud del tratamiento es la protección de un interés esencial para la vida, tal y como destaca el Considerando 46:

"*El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano*".

Asimismo, el citado **Informe 39/2019** analiza un supuesto de cesión de datos derivado de los servicios prestados a través del 112, en relación con el nuevo marco normativo que se deriva del RGPD, y es de especial relevancia

en el caso ahora planteado pues precisamente obedece a conocer cómo afectaría el SAT a la nueva regulación. El citado informe concluye que, en este aspecto no supone novedad alguna en relación con la anterior regulación para lo que cita lo resuelto en el Informe 438/2015 emitido también a raíz de una consulta del CECOES 112 de Canarias:

> (…)La consulta plantea si la comunicación a familiares o allegados de los datos de la asistencia sanitaria prestada y el centro al que ha sido trasladada una persona atendida por el servicio de atención de Urgencias y Emergencias de Canarias (a través de CECOES 112) es conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD), y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RDLOPD). (…)
>
> (…) *en todo caso, de acuerdo con lo dispuesto por el artículo 4.1 de la Ley Orgánica, "Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". También debe recordarse que el artículo 4.2 de la Ley 15/1999 establece que "los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos". Esto implica que los datos tratados o cedidos únicamente podrán ser utilizados en las actividades que* ***se efectúen para resolver la situación de emergencia que motivó la llamada, o la investigación policial para la que se hubieran solicitado los datos, no siendo posible la utilización de tales datos para ninguna otra finalidad****. Por ello, una vez remediada la situación que motivó la llamada de emergencia y la investigación, quienes reciban los datos de los centros de gestión de llamadas de emergencia deberán proceder a su destrucción.* (…)
>
> Esta regla del interés vital consagrada en el artículo 7 d) de la Directiva aparece contenida, al menos parcialmente, en los artículos 7.6 párrafo segundo y 11.2 f) de la Ley Orgánica 15/1999.
>
> Según el primero de los preceptos citados "*también podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior [los datos especialmente protegidos] cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento*".
>
> Añade el artículo 11.2 f) en su primer inciso que será posible la cesión sin contar con el consentimiento del interesado "*cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero*".
>
> (…)

En el supuesto de hecho planteado en la consulta se indica que se reciben llamadas de personas que afirman ser familiares o allegados de una persona atendida por los servicios del 112, para saber si una persona ha sido efectivamente atendida y, en caso afirmativo, el hospital al que ha sido trasladado. Y en este sentido indica la consultante que "cabría analizar si la presencia de este familiar pudiera ser crucial para la vida del paciente, dado que podría conocer de alguna patología importante d éste que fuese necesario trasladar al personal facultativo en el tratamiento a emplear – antecedentes (cardiopatía, diabetes, etc.), alergias (penicilina, etc.)… ". *Es decir, la cesión de datos se efectuaría a una persona que realiza una llamada telefónica al 112 y que se identifica como familiar o allegado de otra persona atendida por los servicios de urgencias y emergencias. Si es el llamante el que identifica al atendido, indicando su nombre y apellidos, pudiera aportar información de interés vital de los atendidos, al facilitar el acceso a datos de salud referidos a aquéllos que pudieran resultar necesarios para prestarles una adecuada asistencia sanitaria. Por tanto, entre estos casos pudieran existir situaciones de urgencia vital, considerando que los familiares o allegados pueden suministrar, en un primer momento de atención médica urgente, información que pudiera resultar esencial para la debida atención en el centro hospitalario de destino, por lo que el supuesto de hecho quedaría incardinado en el interés vital del afectado en esta cesión de los datos.*

Ahora bien, la cesión no implica la comunicación al llamante de cualquier dato de la persona atendida, y menos aún de la concreta asistencia sanitaria prestada. Entendemos que el interés vital quedaría suficientemente garantizado en la medida en que se informara al llamante si la persona ha sido efectivamente atendida por los servicios de urgencias o emergencias – sin indicar la atención médica prestada o la causa probable –, es decir, una respuesta afirmativa o negativa sobre el hecho de haber atendido a una persona concreta, así como el centro hospitalario al que ha sido trasladado; hospital ante el que el familiar o allegado podrán suministrar toda la información relativa a los antecedentes médicos que sea esencial para preservar el interés vital de la persona atendida, aportando datos de salud que pudieran ser imprescindibles para la atención sanitaria urgente y adecuada. Cualquier otra información podría ser excesiva para el cumplimiento de las finalidades previstas, en relación con el art. 4 LOPD antes citado.

(…) *En conclusión, los servicios de urgencias y emergencias podrán comunicar a las personas que llamen identificándose como familiares y allegados de otra que ha sido previamente atendida el dato de si ha sido efectivamente atendida o no, así como del centro hospitalario al que ha sido trasladado, en aplicación de los artículos 7.d) de la Directiva 1995/46/CE y art. 7.6 y 11.2.f) LOPD, concurriendo en estos supuestos*

la causa de interés vital del afectado. Cualquier otra información pudiera ser considerada excesiva en relación con el art. 4 LOPD. (…)

Respecto de la utilización de la base de datos de la CNMC por los servicios de emergencia del 112, el citado **Informe 39/2019** indicaba lo siguiente:

(…)Igualmente, esta Agencia viene fundamentando, reiteradamente, en la necesaria protección de intereses vitales del interesado o de otra persona física, las comunicaciones a las entidades municipales por la Comisión Nacional de los Mercados y la Competencia de los datos de los abonados al servicio telefónico para la prestación del servicio sobre números de abonado en el marco de las llamadas de emergencia, siendo el más reciente el Informe 186/2018:

La consulta plantea si resulta conforme a las normas de protección de datos la comunicación por parte de la Comisión al Ayuntamiento de Marbella, de los datos de los abonados al servicio telefónico para la prestación del servicio sobre números de abonado en el marco de la atención de las llamadas de emergencia.

I

Con carácter general, la comunicación planteada supondrá una comunicación de datos de carácter personal, que deberá fundarse en alguna de las bases jurídicas establecidas en el artículo 6.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos)

Sobre el cumplimiento de la obligación legal de permitir la prestación del servicio de directorio telefónico en condiciones de competencia efectiva y la específica cesión de datos que la misma conlleva, ya se expresó por la Agencia Española de Protección de Datos el criterio de que la misma encontraba tal habilitación legal en la ya derogada Ley 11/1998, de 24 de abril, General de Telecomunicaciones. Así consta en el informe emitido por el Gabinete Jurídico de esta Agencia con fecha 6 de marzo de 2001, habiéndose igualmente emitido informe de fecha 23 de julio de 2002 en relación con el procedimiento para proporcionar tal información por la Comisión del Mercado de Telecomunicaciones a tenor de lo dispuesto en la Orden del Ministerio de Ciencia y Tecnología, de 26 de marzo de 2002, por la que se establecen las condiciones de prestación del servicio de consulta telefónica sobre números de abonado.

En particular, el primero de los informes a los que se acaba de hacer referencia concluía que existía una norma con rango suficiente que habilitaba la mencionada cesión, tomando en consideración lo establecido en los artículos 11.2, 37.1 b) y 54.3 de la derogada Ley General de Telecomunicaciones.

(…)

II

(…) para el supuesto que nos ocupa, la necesaria protección de intereses vitales del interesado o de otra persona física se constituye en la base legítima para la cesión de los datos con información de carácter personal. Por ello, las sucesivas comunicaciones se ampararían, en el régimen vigente desde 25 de mayo de 2018, en el apartado d) del artículo 6.1 del Reglamento General de Protección de Datos.

Este mismo razonamiento puede considerarse aplicable al marco establecido en la vigente Ley 9/2014, de 9 de mayo, General de Telecomunicaciones -LGT-. (…)

Por este motivo, cabe concluir, como ya se hacía en los informes de esta Agencia anteriormente citados que, "*En consecuencia, el legislador viene a concretar expresamente, en una norma con rango de Ley, la posibilidad de que, en un desarrollo reglamentario posterior, se exija a los operadores la aportación de los datos necesarios para dar pleno cumplimiento a los derechos/deberes que él mismo consagra en la propia Ley*. (…)

IV

Centrado así el objeto del debate, tal y como se adelantó anteriormente, se desprende que la comunicación de los datos a la Comisión Nacional de los Mercados y la Competencia al Ayuntamiento de Marbella para la mejor prestación del servicio de emergencias 112, encuentra su fundamento en la necesaria protección de intereses vitales del interesado o de otra persona física.

A su vez, las sucesivas comunicaciones se ampararían, en el régimen vigente desde 25 de mayo de 2018, en el apartado d) del artículo 6.1 del Reglamento General de Protección de Datos.

En conclusión, tal y como se ha expuesto anteriormente, la cesión de Base de Datos de Abonados Telefónicos al Servicio de Emergencias 112 está claramente instrumentada como consecuencia de la obligación, impuesta por la ley, de que dicho servicio identifique la llamada entrante, con determinados datos que se especifican en el Apartado Decimoquinto 2) de la Orden CTE/711/2002, para la atención del servicio de llamada de urgencia.

Así literalmente tanto dicha Orden como la restante normativa citada, especifica que la comunicación de los datos en cuestión es "*para una efectiva prestación de los servicios de atención de llamadas de urgencia*". Tal y como literalmente se expone, tanto en los informes de esta Agencia sobre la cuestión citados en la consulta, como por la normativa, la cesión se ampara en un interés vital del interesado. Es decir, el interés vital del interesado se contempla en la cesión de datos

> de los abonados de los directorios telefónicos como causa legitimadora, de conformidad con las previsiones legales al respecto.
>
> En definitiva, entendemos que la cesión de la Base de Datos de Abonados Telefónicos por la CNMC a los Servicios de Emergencias 112 del Ayuntamiento de Marbella para prestar el servicio de información telefónica para la atención de emergencias -112-, resulta conforme con la normativa de protección de datos.
>
> V
>
> De este modo, la utilización de los datos para una finalidad distinta de la "exclusivamente" prevista por el Ordenamiento podrá dar lugar al inicio de las correspondientes actuaciones por parte de la Agencia Española de Protección de Datos.
>
> Finalmente, se considera adecuada la referencia efectuada por el informe adjunto a la consulta al hecho de que la entidad prestataria del servicio "garantizará el respeto a la legislación vigente en materia de protección de datos conforme a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal y a la libre circulación de estos datos (…), así como a lo establecido en la restante normativa vigente en materia de protección de datos (…), cuya salvaguardia corresponde a la Agencia Española de Protección de Datos".

Teniendo en cuenta lo indicado en los informes que se han venido citando, el criterio de esta Agencia es que el tratamiento de los datos, tanto de localización aportados por los operadores de telecomunicaciones, así como los obrantes en la base de datos de la CNMC, por parte de los servicios de emergencia 112 a los efectos **de atender la llamada y coordinar la intervención** que se estime necesaria, **está basado en el artículo 6.1 d) del RGPD, de acuerdo con la normativa habilitante que se relaciona en los citados informes.**

V

Por lo que si la habilitación del tratamiento de datos de localización *ex articulo 6.1 d) RGPD* **lo es únicamente a los efectos de atender las llamadas que se hayan realizado al 112**, procede analizar la adecuación del SAT al **principio de limitación de finalidad**, previsto en el artículo 5.1 b) RGPD a cuyo tenor, *los datos serán recogidos con fines determinados, explícitos y legítimos, **y no serán tratados ulteriormente de manera incompatible con dichos fines**; («limitación de la finalidad»);*

El Considerando 50 del RGPD indica lo siguiente:

> El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención

de los datos personales. Si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros(…) La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista. Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. (…) En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. (…)

Por su parte, el artículo 6.4 del RGPD establece lo siguiente:

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

De acuerdo con lo expuesto, debe ponerse la atención en que respecto de los datos personales a utilizar por el SAT, se incluyen tanto los de aquellas personas que hayan llamado al 112 como las que no lo hayan hecho. Además respecto de los primeros, debe tenerse en cuenta que la realización de la llamada obedecerá a un supuesto concreto que requiera atención, es decir, obedece a una finalidad concreta y determinada.

Cuestión que no sucede con lo que propone la consultante en la medida en que el funcionamiento del SAT **no parte de la recepción previa de una llamada** sino que en el ejercicio de sus competencias, y al amparo del derecho a la información previsto en el artículo 4 de la Ley de Emergencias de la Comunidad Canaria y las funciones que el artículo tercero apartado j) de la Orden de 21 de diciembre de 1999, atribuye al CECOES, pretende utilizar la información de aquellas personas que han usado el servicio 112, para, motu proprio, el posterior envío masivo de mensajes.

Es decir, aun habiendo realizado una llamada al 112, la utilización que se pretende con el SAT **no es la atención concreta y especifica de la misma**, y que a la sazón **es el único supuesto de hecho que se encuentra habilitado de acuerdo con los informes citados y la normativa estudiada.**

Por lo que menos aún podría considerarse habilitada la utilización de los datos de localización, ya sea a través de la base de datos de la CNMC, ya sea a través de la información que proporcionen los operadores, **de aquellas personas que ni siquiera han realizado llamada alguna al 112.**

El artículo 6.3 del RGPD y el Considerando 50 recoge algunos elementos a tener en cuenta a la hora de realizar el *juicio de compatibilidad* de finalidades, como son relación entre los fines de la recogida y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

En referencia a la **relación entre los fines iniciales y los posteriores, el contexto y las expectativas razonables del interesado**, cabe indicar que el tratamiento que se pretende con el SAT, derivado de que en un momento determinado se haya solicitado los servicios de emergencia, el afectado no puede prever razonablemente que sus datos sean tratados con posterioridad para cuestiones que versen sobre otra materia en general y en un espacio temporal, a priori, indefinido. No por haber utilizado los servicios de atención de emergencias en un momento determinado significa que pueda verse afectado por cualquier tipo de emergencias, máxime teniendo en cuenta los 45 acontecimientos previstos en el PLATECA a los que pretende dar respuesta el SAT.

En relación con las **consecuencias del tratamiento ulterior y la existencia de garantías en el tratamiento**, debe indicarse que teniendo en cuenta la información que aporta la consultante, el respeto al derecho a la protección de datos del sistema en relación con los usuarios de teléfonos móviles, plantea varias dudas.

Por ejemplo, se desconoce si existirán varias versiones de la base de datos que se obtenga de las distintas fuentes, en la medida en que, por ejemplo, una persona realiza una llamada a través de un teléfono móvil al 112 en la isla de La Gomera solicitando atención médica para un familiar, y se le geolocaliza y se almacena dicha información en el sistema. Si con posterioridad dicha persona se ubica en otra isla o incluso ha salido del archipiélago y se produce una situación de emergencia en la isla de La Gomera, tal como está explicado el sistema, recibiría una alerta sobre la situación que se está produciendo, y que en principio no le afectaría. O bien si por el contrario, el sistema haría un seguimiento permanente de su geolocalización para excluirle de esa alerta, lo cual implicaría una grave injerencia en su privacidad y en la libertad de movimientos.

Se desconoce, por tanto, si el sistema se actualizaría y de qué modo para evitar situaciones como las del ejemplo. Es decir, se desconoce durante cuánto tiempo se almacenan y si se van eliminando los registros que no son necesarios en la medida en que ya no sirvan al cumplimiento de la finalidad del sistema y en base a qué requisitos pueden considerarse así.

Finalmente y también relacionado con la existencia de garantías, nada se indica en la explicación del funcionamiento del SAT sobre el ofrecimiento de información previa a los usuarios respecto del posterior tratamiento de sus datos. Por consiguiente, los datos únicamente podrán emplearse para los fines que justifican esa recogida y, de los que habrá debido ser informado el afectado, cuestión respecto de lo que nada se indica en la consulta, no siendo lícito el uso para otros fines.

En cuanto a la utilización de los datos de localización obtenidos a partir de la dirección administrativa que consta en la base de datos de la CNMC, a los efectos pretendidos por el SAT, de personas que ni siquiera han utilizado los

servicios del 112, resulta innecesario, por obvio, el juicio de compatibilidad de finalidad, siendo la respuesta negativa.

De acuerdo con lo expuesto, la utilización de los datos personales de los usuarios de los servicios de emergencias del 112, como de los que no han usado dichos servicios, ya sea a través de la información que aportan los operadores de telecomunicaciones, ya sea a través de la base de datos de la CNMC, por el SAT, resulta contraria al principio de finalidad.

VI

En relación con el principio de limitación del plazo de conservación, previsto en el artículo 5.1 e) del RGPD a cuyo tenor *los datos serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales*; (…) («limitación del plazo de conservación»); respecto del sistema SAT y los posibles orígenes de los datos a tratar, tal como se ha indicado antes, **se desconoce por cuanto tiempo serian tratados los datos que pretende utilizar y si existe algún criterio para determinar que los mismos ya no sirven a la finalidad pretendida**.

VII

De acuerdo con lo expuesto, son de aplicación al presente caso las conclusiones a las que se llegó en el **Informe 71/2013**, que cita la consultante y que versa sobre un sistema de alerta propuesto por la Comunidad Autónoma de Andalucía, similar al SAT.

> (…)**la cesión de Base de Datos de Abonados Telefónicos al Servicio de Emergencias 112 está claramente instrumentada como consecuencia de la obligación**, impuesta por la ley, de que dicho **servicio identifique la llamada entrante**, con determinados datos que se especifican en el Apartado Decimocuarto de la Orden CTE/711/2002, para la atención del servicio de llamada de urgencia. Así literalmente tanto dicha Orden como la restante normativa citada, incluso con subrayado por nosotros, en el apartado II, especifica que la comunicación de los datos en cuestión es "**para una efectiva prestación de los servicios de atención de llamadas de urgencia**". (…)
>
> Es decir, el interés vital del interesado se contempla en la cesión de datos de los abonados de los teléfonos fijos como causa legitimadora, pero para la identificación de la concreta llamada entrante, definiendo el lugar de procedencia y otras cuestiones, pero no previendo que ello implique definir un número – como decíamos más arriba, indeterminado – de abonados por una – como decíamos también antes, indeterminada – calamidad o catástrofe. Es decir, la cesión de la Base de Datos de

Abonados Telefónicos **está prevista para una finalidad de satisfacer intereses vitales de interesados determinados** – los llamantes – **de conformidad con las previsiones legales al respecto.** Otra cosa muy distinta sería que exista un interés vital diferente, de otros abonados, en conocer una incidencia, catástrofe o calamidad pública, que pueda afectarles, poniendo medidas para ello.

Entendemos que se trata de **un ámbito que excede con creces del tema de los fines compatibles** previsto en el art. 6.1.b) de la Directiva 95/46/CE y art. 4.2 LOPD. En este punto es interesante mencionar el reciente documento del Grupo de Trabajo del Art. 29 de la Directiva 95/46/CE sobre la cuestión. Se trata de la Opinión 3/2013 sobre la limitación de finalidades – aún disponible sólo en ingles, denominado "Purpose limitation", que versa también sobre los fines compatibles al ser conceptos íntimamente relacionados. Tal y como indica el apartado II.3 del documento, en los fines compatibles cobra especial relevancia la predictibilidad por parte de los afectados; es decir, que los interesados pudieran fácilmente predecir, según los fines originarios de sus datos sobre los que fueron informados, que los mismos se utilizarán para otros fines compatibles por su estrecha relación con los primeros. Y dicho documento ofrece ulteriores criterios para determinar si los fines son compatibles o no, como puede ser no sólo la predictibilidad para el afectado, titular de los datos, sino también la relación entre los fines, el contexto y las expectativas razonables de los interesados, la naturaleza de los datos y el impacto en la protección de datos en caso de uso para fines ulteriores compatibles y las salvaguardas y medidas impuestas por el responsable de fichero.

Pues bien, bajo **ninguna de estas perspectivas encontramos que la respuesta a grandes emergencias pudiera ser un fin compatible**. La normativa expuesta, reiteramos, que en este punto entronca con las legítimas expectativas del sujeto, implica que el fin primario de la identificación de la llamada por el Servicio de Emergencias 112 es la atención de dicha llamada. La gestión de grandes emergencias es un tema lo suficientemente importante como para tener su identidad propia, y así es una materia sometida a la elaboración de planes que ya prevé la Ley de Protección Civil. Tampoco se determinan por **el consultante salvaguardas o medidas para asegurar que en caso de uso para el fin propuesto el nuevo tratamiento será equitativo y que no producirá efectos perjudiciales en los sujetos, como podría ser en caso de ser alertados de emergencias que no les afectaran, por ejemplo**. Y es que en definitiva la cesión de los datos en cuestión por parte de la antigua Comisión del Mercado de las Telecomunicaciones está tan delimitada en lo que a su finalidad se refiere, y se trata de datos tan importantes, que **la finalidad pretendida entendemos que se erige como independiente**. Si pretendiera establecerse el sistema en cuestión, debería realizarse expresamente, con su propia causa

legitimadora – también el interés vital, pero no del interesado llamante, sino de la población afectada por determinada catástrofe - , **y con su propia normativa reguladora que estableciera autoridades competentes, condiciones de uso y requisitos, así como los mecanismos de seguridad aplicables**.

Además, tal y como resulta del Apartado II del presente informe, el ordenamiento jurídico **ya prevé otros sistemas de difusión masiva de alertas ante grandes emergencias, y así estará previsto en los planes correspondientes, como es la utilización para tal fin de los medios de comunicación social.** Nos referimos al art. 6 de la Ley 2/1985 y a los correlativos preceptos de la legislación autonómica antes citados. Es decir, el ordenamiento ya prevé un sistema de difusión masiva de alertas, y lo atribuye a determinados órganos, sin que por tanto el supuesto de hecho planteado esté desprovisto de una respuesta legal. (…).

En definitiva, entendemos que la cesión de la Base de Datos de Abonados Telefónicos por la CMT a los Servicios de Emergencias 112 está prevista para **una finalidad claramente determinada, que es la identificación y consiguiente atención de la emergencia de la llamada entrante, sin que pueda entenderse que la difusión masiva de alertas es un fin compatible con el anterior, sino que se trataría de una finalidad diferente que por tanto debe encontrar su amparo en su propia legitimación**.

V

En cuanto a los teléfonos móviles, se plantea un sistema de difusión masiva de alertas a través de la geolocalización de los terminales, suponemos que únicamente estén ubicados en una zona afectada por la emergencia, aunque nada se dice al respecto. Como indicábamos anteriormente, tampoco se nos específica sobre el sistema de geolocalización a determinar.

Pues bien, entendemos que la utilización de un sistema de geolocalización, sea mediante triangulación mediante los datos procedentes de las estaciones de base, sea mediante GPS o redes WiFi, debería estar expresamente previsto en la normativa, bien como causa legitimadora para la cesión de tales datos, bien como obligación de los operadores para satisfacer un interés vital de los interesados, o ser expresamente consentida por los usuarios.

(…)

Decimos esto porque la Ley General de Telecomunicaciones prevé la cesión del dato de la localización del terminal en el artículo 33, obligando a los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público al agente facultado (art. 33.5.i, 33.6 y 33.7 LGTel.). Fuera de estos casos, **sólo se permite a los operadores el**

tratamiento de los datos de localización con el consentimiento de los usuarios y para la prestación de los servicios de valor añadido, previéndose como uno de los derechos de los consumidores y usuarios finales. (…)

Por tanto, la legislación **no impone a los operadores de servicios de telecomunicaciones la obligación de cesión de los datos de localización para la gestión de grandes emergencias, ni siquiera de modo genérico o indiciario**. Al contrario, prevé que tales datos sólo puedan tratarse con dos requisitos: que sean para la prestación de servicios de valor añadido y con el previo consentimiento de los interesados. Puesto que tales premisas no concurren en el supuesto planteado, no encontramos base legal suficiente para imponer a los operadores la obligación pretendida. (…)

Del citado informe se extraen **las siguientes conclusiones que son predicables del SAT propuesto por la consultante**:

(i) el uso de la base de datos que proporciona la CMT (actual CNMC) por parte de los servicios de emergencias, responde únicamente a la finalidad de identificar y atender la llamada de aquellas personas que llamen al 112. También reclama que en la consulta que se planteó, no se indican salvaguardas a fin de evitar que determinados usuarios del 112 reciban alertas que en principio no les afecten.

(ii) el tratamiento de datos personales debe observar el principio de limitación de finalidad, para lo que se cita el Dictamen 3/2013 sobre limitación de finalidad del Grupo de Trabajo del articulo 29 (actualmente sustituido por el CEPD), a los efectos de entender que el sistema de envíos masivos, a los destinatarios que hayan utilizado el teléfono de emergencia 112, obedece a una finalidad incompatible y que se erige independiente.

(iii) el ordenamiento jurídico ya prevé otros sistemas de difusión masiva de alertas ante grandes emergencias, y así estará previsto en los planes correspondientes, como es la utilización para tal fin de los medios de comunicación social.

VIII

Finalmente procede analizar la tercera fuente de obtención de los datos que pretende utilizar el SAT, es decir, la información de aquellos usuarios que han descargado e instalado **la aplicación para dispositivos móviles de emergencias** establecida al efecto (la app112 en lo sucesivo).

Se realiza el siguiente análisis de manera separada de las anteriores posibles fuentes de datos, en la medida en que ahora **se requiere ineludiblemente la acción consciente por parte de los titulares de los**

datos, circunstancia que dota a esta categoría de importantes diferencias e implicaciones en los principios de licitud y finalidad en el tratamiento de los datos, respecto de lo indicado hasta ahora.

Como punto de partida debe indicarse que se desconoce en qué términos se informa al usuario de la app112 sobre la **finalidad** de la misma y respecto **de qué datos** se someten a tratamiento, no obstante en la medida en que se promociona a través del CECOE 112 se puede deducir, que en términos generales, la finalidad irá dirigida a establecer comunicación con el citado organismo a los efectos de requerir intervención en caso de emergencia y en su caso**, a estar informados respecto de posibles situaciones de emergencia, ya sea a través de alertas o la recepción de mensajes** (pues sin este servicio de "recepción de información" no tendría sentido la app112 ya que no diferiría del servicio ordinario de atención a emergencias tras realizar una llamada al 112).

En primer lugar debe acudirse al artículo 6 del RGPD antes citado para encontrar una base jurídica que de licitud al tratamiento.

El apartado 1.a) considera licito el tratamiento cuando, *el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos*;

Por su parte, el artículo 4.11 del RGPD considera «consentimiento del interesado»: *toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;*

El artículo 7 del RGPD sobre "Condiciones para el consentimiento" dispone lo siguiente:

> *1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.*
>
> *2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.*
>
> *3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.*
>
> *4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se*

supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

En el presente caso y sobre la premisa de que la finalidad a la que sirve la app112 es tanto, ponerse en contacto con el servicio de emergencias, **como recibir avisos o alertas sobre posibles situaciones de emergencia**, debe obtenerse el consentimiento del usuario mediante una clara acción afirmativa de modo que el responsable pueda demostrar que cuenta con el mismo, y garantizando la posibilidad de revocarlo.

Asimismo debería analizarse cuales son los datos son necesarios para la prestación del servicio en cuestión, y en caso contrario, otorgar la posibilidad de seguir prestando el mismo sin el tratamiento de aquellos.

Fuera de este supuesto, esto es, si a tenor de lo indicado en el Considerando 294 de la Directiva 2018/1972 antes citado, se establece un sistema de alerta pública que no descanse en el consentimiento, deberá regularse una norma con rango de ley, respetando el principio de proporcionalidad y estableciendo las garantías oportunas, para que sea conforme al artículo 6.1.e) del RGPD y al artículo el 8.2 LOPDGDD que dispone que:

El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

En este sentido, no puede considerarse suficiente la regulación prevista en la Ley 9/2007, de 13 de abril, del Sistema Canario de Seguridad y Emergencias, pues ni en su artículo 37 invocado por la consultante – y que se remite a los medios de comunicación social para lograr el fin pretendido – ni en el resto del articulado, se establecen referencias en este sentido, que amparen el tratamiento que se pretende con la implantación del SAT tal como se describe en la consulta.

Por otro lado debe indicarse que estamos ante un tratamiento que puede requerir de diversos datos con implicaciones diferentes sobre todo en lo que se refiere al **derecho de información y al principio de transparencia.** Una cosa son los datos identificativos, como podrán ser nombre, apellidos y nº de línea (que pueden considerarse a estos efectos estáticos, en la medida en que siempre serán los mismos) y otros son datos que también, son identificativos pero que por su naturaleza y el contexto del uso de la app112 son cambiantes.

Estos son los datos de geolocalización, en la medida en que el usuario puede realizar desplazamientos a lo largo del ciclo de uso de la aplicación, y por tanto no serán los mismos, aquellos que se recogieron cuando se instaló la misma, y aquellos que, por ejemplo, se recaben en otro momento posterior, lo

que requiere un complemento informativo para dar cumplimiento al principio de transparencia (art. 12 RGPD) y al derecho a la información (art. 13 del RGPD).

Establece el artículo 12 del RGPD, sobre " Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado" lo siguiente:

> *1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.*
>
> *2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.*
>
> *(…)*
>
> *7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.*
>
> *(…)*

En este sentido, nos indica el Considerando 58 del RGPD lo siguiente: *El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea.*

Por su parte, el Considerando 60 dispone que: *Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea*

necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. (…) Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente.

Establece el artículo 13 del RGPD lo siguiente:

> *1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:*
>
> > *a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;*
> >
> > *b) los datos de contacto del delegado de protección de datos, en su caso;*
> >
> > *c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;*
> >
> > *d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;*
> >
> > *e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;*
> >
> > *f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.*
>
> *2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:*
>
> > *a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;*
> >
> > *b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;*

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Teniendo en cuenta lo anterior y sobre la base que estamos ante la recogida y uso (tratamiento) de dos clases o categorías de datos, aquellos ordinarios o estáticos y aquellos cambiantes, en el uso de la app112 a los efectos del SAT, deberán facilitarse respecto de los primeros, aquella información que consta en el artículo 13 RGPD arriba transcrito y respecto de los datos de geolocalización, en la medida en que se recogen y se tratan en varios momentos distintos a la instalación de la app112, deberá complementarse la información de que, efectivamente, se está produciendo la recogida de éste tipo de datos, ya sea a través de iconos o avisos en el dispositivo en cuestión o a través de otros medios.

Sobre esta cuestión en la Resolución de 10/06/2019, recaída en el Procedimiento Nº: PS/00326/2018, se analizaba la adecuación al principio de transparencia de una aplicación para dispositivos móviles, que recogía, entre otros datos, **la geolocalización**, la AEPD resolvió lo siguiente:

Establece el artículo 5 del RGPD bajo la rúbrica "Principios relativos al Tratamiento", en su apartado 1 a) lo siguiente: 1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el

interesado («licitud, lealtad y transparencia»); (el subrayado es de la Agencia Española de Protección de Datos).

El tratamiento de datos que se realiza a través de la aplicación (…) , en los dispositivos de usuarios, derivado de la funcionalidad del micrófono y la geolocalización, vulnera el principio de transparencia previsto en el artículo 5.1 del RGPD, tal como se expone a lo largo de la presente resolución. En apoyo a esta afirmación debe acudirse a los siguientes elementos:

En primer lugar, los Considerandos 39 y 60 del RGPD determinan lo siguiente: (…) Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. (…) (El subrayado es de la Agencia Española de Protección de Datos).

Y (…) Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. (…) (El subrayado es de la Agencia Española de Protección de Datos).

*Como puede observarse, el texto del Considerando 39 utiliza verbos en su forma presente, de modo que **en el momento en el que** se están recogiendo, utilizando, consultando o tratando la información captada por el micrófono y la geolocalización, - que obviamente no sucede cuando se instala la aplicación y se aceptan los tratamientos en un primer momento- **se hace necesario esa información adicional**, como podría ser, por ejemplo, una viso en forma de icono o marca, que permitiera al usuario conocer ese tratamiento "a tiempo real", que serviría para complementar la información que se recibió inicialmente, habida cuenta del contexto especifico en el que se trata la información (Co. 60).*

*(…)Sentado lo anterior, y en relación con el contexto especifico y las características del tratamiento que le hacen acreedor de esa adaptación y complementariedad informativa, debe ponerse de manifiesto **como punto de partida**, que los dispositivos móviles (tablets y smartphones) son dispositivos que se caracterizan por sus múltiples funcionalidades, ya que son ampliamente utilizados tanto como teléfonos, agendas, cámaras, así como para el acceso a Internet. Además, la posibilidad de instalación de aplicaciones en estos dispositivos amplía prácticamente sin límite estas funcionalidades, haciendo muy difícil al usuario recordar todos los consentimientos o*

permisos que ha otorgado en cada una de las aplicaciones instaladas, así como su gestión.

Siendo los teléfonos móviles dispositivos que sus usuarios ***acostumbran a portar con ellos de forma continua y generalizada****, el hecho de la posible activación del micrófono y de la ubicación de estos dispositivos* ***puede llevar a generar situaciones de alarma entre los usuarios, que entienden que pueden estar siendo vigilados en todo momento****. Ello* ***intensifica la necesidad de facilitarles información complementaria para garantizar un tratamiento transparente****, que debería incluir el alcance de dicho tratamiento (cómo y cuándo), e informar "a tiempo real" que se está utilizando el micrófono y la geolocalización.*

(…)En segundo término, como se ha indicado antes, ***debe tomarse en consideración que*** *estamos ante un tratamiento que no se produce inmediatamente después de prestar el consentimiento, sino que la recogida de los datos, y las restantes acciones objeto de tratamiento pueden llevarse a cabo, con muy alta probabilidad, en un momento separado en el tiempo.*

(…)Ese lapso entre la aceptación de las funcionalidades descritas y el momento en el que, efectivamente se produce el tratamiento, (…) hace necesario esa adaptación del principio de transparencia a este tipo de tratamiento, siendo indispensable informar con certidumbre y transparencia acerca de cuándo se producirá el tratamiento- tanto en el momento de la instalación de la aplicación, como durante la recogida de información -, en particular en aquellos más intrusivos como son la captación de sonidos por el micrófono y la geolocalización.

(…) precisamente para no establecer una diferenciación entre los modos de informar y por las múltiples posibilidades de diferentes espacios temporales entre la proporción de la información respecto del uso de micrófono y geolocalización y la verdadera captación, se hace necesario que se informe en el momento en que se está produciendo dicha captación.

(…)_En este sentido resulta especialmente clarificador, en relación con el caso analizado, lo recogido en el documento Dictamen GT260, de 29 de noviembre de 2017 relativo a Directrices sobre la Transparencia en virtud del Reglamento 2016/679 elaborado por el Grupo de Trabajo del Articulo 29 –y ratificado por el Comité Europeo de Protección de Datos- , indica en su apartado 39 lo siguiente (…) Otra forma posible de proporcionar información de transparencia es mediante el uso de avisos «push» y «pull». Los avisos «push» implican la provisión de avisos de información de transparencia ad hoc, mientras que los avisos «pull» facilitan el acceso a la información mediante métodos tales como administración de permisos, paneles de privacidad y tutoriales de «más información». Estos permiten una experiencia de

transparencia más centrada en el usuario para el interesado. (…) (El subrayado es de la Agencia Española de Protección de Datos). También debe indicarse que el citado documento en su apartado 43 indica lo siguiente (…) El considerando 78 se refiere a los responsables del tratamiento que aplican medidas que cumplen los requisitos de protección de datos desde el diseño y por defecto, incluidas medidas consistentes en la transparencia con respecto a las funciones y el tratamiento de los datos personales (…) (El subrayado es de la Agencia Española de Protección de Datos).

(…)Este refuerzo o recordatorio del consentimiento prestado en el momento de descargarse la aplicación obedece a la circunstancia de que no puede ser igual, ni sujeto a las mismas formalidades, el consentimiento prestado en un momento dado para que un responsable recopile unos determinados datos y solo esos datos, que el consentimiento prestado para que el responsable pueda en cualquier momento, recopilar datos que por su propia naturaleza son cambiantes o dinámicos , como por ejemplo sucede con los de geolocalización (es de muy alta probabilidad que la ubicación cambie respecto del momento en que se otorga el consentimiento, al momento en que se recogen los datos), que en sí mismos no son "un dato" sino una categoría de datos, siendo ajeno a esta circunstancia el propio afectado, de tal modo que el principio de transparencia ***reclama un recordatorio, marca o señal de que se está produciendo el tratamiento en ese preciso momento temporal y espacio físico que se suceda cuando se activen las citadas funcionalidades.***

(…)Por todo ello, el tratamiento analizado reclama un especial refuerzo del principio de transparencia - en relación con la proporcionalidad del tratamiento- en todas sus manifestaciones y con garantías adecuadas en relación con el tipo de tratamiento,

De acuerdo con lo expuesto, deberá **informarse** a los usuarios de la app112 en los términos del artículo 12 del RGPD y con el contenido mínimo del artículo 13 del RGPD en el momento de descargar e instalar la misma para ser receptores de los avisos del SAT.

Y deberá darse cumplimiento al **principio de minimización** y **limitación de finalidad** en la medida en que los datos objeto de tratamiento serán estrictamente **los necesarios** para cumplir la finalidad pretendida y su uso debe responder únicamente al cumplimiento de la misma, no pudiendo comunicarlos a terceros ni usarlos para otras finalidades a no ser que se haya aceptado expresamente por los usuarios.

Sobre la circunstancia de que sean necesarios debe indicarse que la evaluación de lo que es **«necesario»** implica una evaluación conjunta y factual del tratamiento y del objetivo «en relación con el objetivo perseguido y de si es menos intrusiva que otras opciones para alcanzar el mismo objetivo». **Si existen alternativas realistas, menos intrusivas, el tratamiento no es**

«necesario»(*TJUE en el asunto Rigas, en el que declaró que «por lo que se refiere al requisito relativo a la necesidad de tratar datos personales, debe tenerse en cuenta que las excepciones y limitaciones en relación con la protección de datos personales deben aplicarse únicamente en la medida en que sea estrictamente necesario». TJUE, asunto C-13/16, Valsts policijas regionalia Rigas regiona parvaldes KartIbas policijas, Rigas pasvaldIbas SIA «Rigas satiksme», apartado 30*).

Se hace esta indicación en la medida en que si entre las funciones de la app112 se encuentra recibir avisos sobre emergencias podrían darse al menos dos alternativas, el envío de mensajes a la totalidad de los usuarios de la app112 o el envío de mensajes únicamente a aquellos que se encuentren en zonas de riesgo. Es decir, dependiendo que alternativa se tenga en cuenta, el uso de los datos de geolocalización no resultaría necesario, pues bastaría con el nº de línea en cuestión para enviar los mensajes.

Respecto de los datos de geolocalización (utilizados para poder ser identificados en lugares dónde se esté produciendo la situación de emergencia), **deberá informarse mediante iconos o avisos, en el dispositivo móvil, cuando se esté captando la información sobre la ubicación**, sin perjuicio de haber obtenido el consentimiento previo e informado y con independencia de haber configurado el dispositivo mediante los parámetros del sistema operativo que utilice.

Respecto de estos últimos, y su recogida en un momento posterior, no es necesario informar de otros aspectos que recoge el art. 13 del RGPD, tanto por cuestiones prácticas que implicarían cada vez que se recoge la ubicación mostrar la totalidad del contenido del art. 13 RGPD), como porque así lo indica el apartado 4 del citado precepto, en la medida en que con la instalación inicial de la aplicación los usuarios **ya han sido informados**.

En definitiva, lo que se pretende con este complemento informativo, es **que el usuario conozca que en ese momento se está accediendo a sus datos de geolocalización y se están enviando,** para si lo desea, desactivar esa funcionalidad del dispositivo (incluso revocando el permiso de la aplicación en el sistema operativo), revocar el consentimiento o desinstalar la aplicación, todo ello en aras a reforzar el *poder de disposición y control* sobre los datos que se configura como una pieza fundamental del elenco de las facultades que integran el derecho fundamental a la protección de datos (STC 292/2000, de 30 de noviembre).

Por lo tanto, **seria conforme a la normativa de protección de datos, el uso de la información de los usuarios de la app112 para ser receptores de los envíos masivos del SAT, siempre y cuando se haya recabado el consentimiento de los afectados en los términos previstos los artículos 7, 12 y 13 del RGPD, y con las adaptaciones necesarias en relación con el contexto en que se recaban y transmitan los datos personales, en especial, los de geolocalización.**

X

Por otro lado, tal y como viene señalado reiteradamente esta Agencia y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”.

Directamente relacionado con el principio de responsabilidad proactiva recogido en el artículo 5.2. del RGPD se encuentra el principio de protección de datos desde el diseño y por defecto que se recoge en el artículo 25 del RGPD:

> *1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.*
>
> *2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.*
>
> *3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.*

Para el adecuado cumplimiento de dicho principio, el RGPD contempla una serie de instrumentos que permiten a responsables y encargados valorar el riesgo que pueda implicar el tratamiento y adoptar las medidas que procedan.

En primer lugar, resulta necesario realizar el **análisis de riesgos** al que se refiere el artículo 24 del RGPD:

> *1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.*
>
> *2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.*
>
> *3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.*

Asimismo, y en relación con los datos de geolocalización respecto de los que se deduce que son fundamentales para el funcionamiento del SAT debe indicarse que el RPGD establece garantías adicionales cuando se pretenda realizar un tratamiento de datos personales como el descrito en la consulta.

El artículo 35 del RGPD establece lo siguiente:

> *1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.*
>
> *2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.*
>
> *3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:*
>
> > *a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;*

> *b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o*
>
> *c) observación sistemática a gran escala de una zona de acceso público.* (…)

En las Directrices WP248 de 4 de octubre de 2017 del GT29 "*sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*, se clarifican varios conceptos que deben tenerse en cuenta en el supuesto objeto de la presente consulta:

> (…)*3. Observación sistemática: tratamiento usado para observar, supervisar y controlar a los interesados, incluidos los datos recogidos a través de redes u «observación sistemática [...] de una zona de acceso público» [artículo 35, apartado 3, letra c)]15. Este tipo de observación representa un criterio porque los datos personales pueden ser recogidos en circunstancias en las que los interesados pueden no ser conscientes de quién está recopilando sus datos y cómo se usarán. Además, puede resultar imposible para las personas evitar ser objeto de este tipo de tratamiento en espacios públicos (o espacios de acceso público).*

El GT29 interpreta «sistemática» en uno o más de los siguientes sentidos (véanse las Directrices del GT29 sobre el delegado de protección de datos, 16/EN WP 243):

- que se produce de acuerdo con un sistema;
- preestablecido, organizado o metódico;
- que tiene lugar como parte de un plan general de recogida de datos;
- que se lleve a cabo como parte de una estrategia.

Asimismo, el GT29 interpreta «zona de acceso público» como cualquier sitio abierto a cualquier persona, por ejemplo, una plaza, centro comercial, calle, mercado, estación de tren o biblioteca pública

En el caso del funcionamiento del SAT estos conceptos cobran especial relevancia teniendo en cuenta que se pretende identificar la ubicación de los usuarios de la app112 para contrastarla con la localización de un evento que suponga un riesgo de emergencia y enviar los avisos que consideren adecuados. Por lo que indudablemente el SAT **realizaría una observación sistemática de los usuarios en relación con su ubicación en zonas de acceso público dónde se vayan a producir o se estén produciendo situaciones de emergencia.** Sin perjuicio de que para la efectividad del sistema también se realizaría en otras zonas – ajenas al espacio público- dónde se lleven a cabo actos de la esfera privada de las personas.

Continua el citado Dictamen analizando que se entiende por (…)*5. Tratamiento de datos a gran escala: el RGPD no define qué se entiende por gran escala, aunque el considerando 91 ofrece alguna orientación. En cualquier caso, el GT29 recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala:*

a. el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;

b. el volumen de datos o la variedad de elementos de datos distintos que se procesan;

c. la duración, o permanencia, de la actividad de tratamiento de datos;

d. el alcance geográfico de la actividad de tratamiento.

En el caso del SAT no puede obviarse que los usuarios finales de los mensajes masivos de avisos de emergencias serian toda la población que se encuentre en el archipiélago canario, y que **no se ha concretado ni en la consulta ni en el informe que se adjunta a la misma, la duración o permanencia de la actividad de tratamiento de datos.**

Por último, el Dictamen indica sobre la necesidad de realizar la EIPD que (…)*En la mayoría de los casos, un responsable del tratamiento puede considerar que un tratamiento que cumpla dos criterios requerirá la realización de una EIPD. En general, el GT29 considera que cuantos más criterios cumpla el tratamiento, más probable será que represente un alto riesgo para los derechos y libertades de los interesados y, por tanto, requiera una EIPD independientemente de las medidas que el responsable contemple adoptar.(…)*

De acuerdo con lo expuesto, y con independencia del origen de los datos personales que vayan a someterse a tratamiento, para la puesta en funcionamiento del SAT se requerirá la realización de una evaluación de impacto en los términos del artículo 35 del RGPD.

Siendo las garantías por adoptar las que resulten del correspondiente análisis de riesgos y de la propia evaluación de impacto y que deberá valorar el responsable del tratamiento, en el presente caso, el CECOES112 o el departamento que pretenda implantarlo, debidamente asesorado por su delegado de protección de datos.

Además, deberá consultar a la autoridad de protección de datos competente antes de proceder al tratamiento cuando la evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo (artículo 36), salvo que el responsable sea capaz de garantizar que el riesgo puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación (Considerando 94 del RGPD).