

CNS 19/2020

**Dictamen en relación con la consulta formulada por un ayuntamiento sobre la posibilidad de utilizar la base de datos SGDA de la CNMT para avisar a la población en casos de emergencias graves.**

**Se presenta ante la Autoridad Catalana de Protección de Datos una solicitud de dictamen de un ayuntamiento sobre la posibilidad de utilizar los datos de la base de datos del Sistema de gestión de datos de abonados (SGDA) facilitada por la CNMT para avisos a la población en casos de emergencias graves.**

**Analizada la consulta, que se acompaña de la resolución de la CNMT de 15 de septiembre de 2009 que estima la solicitud del Ayuntamiento de acceder a la mencionada base de datos para facilitar los datos de abonados previstos en el Orden ministerial de 26 de marzo de 2002 para prestar el servicio de atención a llamadas de urgencia a través del número 092, y en la que se detallan las condiciones del contrato de cesión de datos al Ayuntamiento, de acuerdo con el informe de la Asesoría Jurídica emito el siguiente dictamen:**

(...)

II

**En la consulta se expone que la CNMT facilita al ayuntamiento, de forma periódica, información de la base de datos llamada Sistema de Gestión de Datos de Abonados (SGDA) para la gestión del sistema de atención de emergencias 092 de la Guardia Urbana, de acuerdo con la resolución de la CNMC de 15 de septiembre de 2009**

**Según indica, esta base de datos contiene los números de teléfono móviles y fijos y el nombre y apellido de cada uno de los titulares de la línea asociada al citado número y perteneciente al ámbito de actuación del Ayuntamiento. Esta información se introduce en el sistema de información de atención a la Guardia Urbana de tal modo que cuando desde algún teléfono se llama al 092, el sistema muestra el número de teléfono y su titular para gestionar la emergencia.**

**Asimismo expone que, ante las situaciones de alerta que se están viviendo en la actualidad, el ayuntamiento analiza la posibilidad de utilizar esta base de datos “como medio para hacer llegar avisos mediante SMS o llamadas, a la población en casos de emergencia y excepcionales (avisos de confinamiento, situaciones graves que puedan poner en peligro la vida de las personas u otras situaciones de carácter similar como podría ser la pandemia del Covid-19 o el producido en la petroquímica de Tarragona) , por tanto, limitado a casos de emergencia y excepcionales**

**En este contexto, plantea a esta Autoridad las siguientes cuestiones:**

- “1. ¿Se podrían tomar en consideración como bases legitimadoras para la citada finalidad las previstas en el artículo 6.1 d) y/oe) del RGPD sin necesidad de obtener el previo consentimiento del titular de la línea?”**
- 2. ¿Se podrían considerar suficientes alguna de las dos bases legitimadoras indicadas anteriormente para realizar estos avisos, siempre previa aprobación de su uso por el Comité de Emergencias del Municipio en cuestión?**
- 3. Adicionalmente, ¿podría incorporar esta forma de aviso a la población en el nuevo Documento único de protección civil municipal (DUPROCIM) que se quiere aprobar en el municipio?**
- 4. ¿Sería necesario habilitar una aplicación móvil o web para que los ciudadanos se dieran de alta?**
- 5. Teniendo en cuenta que todavía no se ha transpuesto por parte del gobierno español el Código Europeo de Comunicaciones Electrónicas, siendo la fecha límite para transponerlo el 21 de junio de 2022. Hasta su efectiva transposición se podría utilizar este sistema de aviso mediante SMS o llamada únicamente por los ciudadanos del municipio?”**

### III

Para responder a la primera de las cuestiones planteadas, hay que tener en consideración que, de acuerdo con el Reglamento (UE) 2016/679, del Parlamento y del Consejo Europeo, de 27 de abril de 2016, General de Protección de Datos (en adelante, RGPD) cualquier tratamiento de datos personales, entendido como “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, coteo o interconexión, limitación, supresión o destrucción.” (artículo 4.2 RGPD), debe someterse a los principios y garantías establecidos por aquel Reglamento.

El RGPD define dato personal como: “toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un número, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;” (artículo 4.1 RGPD). Parece claro, pues, que en la medida en que las personas abonadas sean personas físicas, los datos que constan en la base de datos SGDA deben considerarse información personal y están sometidos a la normativa de protección de datos.

El artículo 5.1.a) del RGPD establece que todo tratamiento de datos personales debe ser lícito, leal y transparente en relación con el interesado (principio de licitud, lealtad y transparencia).

Para que un tratamiento sea lícito es necesario contar con, al menos, una base jurídica de las previstas en el artículo 6.1 del RGPD que legitime este tratamiento, ya sea el consentimiento de la persona afectada, ya sea alguna de las demás circunstancias que prevé el mismo precepto:

“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 se parte o para la aplicación a petición del mismo 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 derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. (...)”

En el ámbito de las administraciones públicas, resultan de especial interés, las bases jurídicas previstas en las letras c) y e) del artículo 6.1 del RGPD, según las cuales el tratamiento será lícito cuando sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento (letra c), o cuando el tratamiento sea necesario para el cumplimiento de un interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (letra e).

Ahora bien, tal y como se desprende del artículo 6.3 del RGPD, la base jurídica del tratamiento indicado en ambos casos debe estar establecida por el Derecho de la Unión Europea o por el derecho de los Estados miembros que se aplique al responsable del tratamiento.

La remisión a la base legítima establecida conforme al derecho interno de los Estados miembros requiere, en el caso del Estado Español, de acuerdo con el artículo 53 de la Constitución Española, que la norma de desarrollo, por tratarse de un derecho fundamental, tenga rango de ley.

En este sentido, el artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales establece el rango de ley de la norma habilitante.

En el caso que nos ocupa, el Ayuntamiento plantea si la utilización de estos datos puede ampararse en la letra d) (protección de intereses vitales) y/o en la letra e) (cumplimiento de una misión en interés público).

Así pues, a fin de determinar si las previsiones de las letras d) o e) del artículo 6.1 RGPD pueden constituir una base legítima del tratamiento de datos efectuado por el Ayuntamiento con la

finalidad de comunicación a su población en casos de emergencia y excepcionales (avisos de confinamiento, situaciones graves que puedan poner en peligro la vida de las personas u otras situaciones de carácter similar como podría ser la pandemia del Covid-19 o el producido en la petroquímica de Tarragona), será necesario analizar si se dan las circunstancias que justifican el tratamiento en base a la protección de intereses vitales del interesado u otra persona física o si el ayuntamiento actúa en ejercicio de una misión en interés público o de poderes públicos conferidos por una norma con rango de ley tal y como exige el artículo 6.3 RGPD.

#### IV

En cuanto a la protección de intereses vitales del interesado o de otra persona física, el considerante 46 del RGPD precisa que:

“El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial por la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse en base al 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”

Así, se pone de manifiesto que determinados tipos de tratamiento pueden responder tanto a motivos de interés público como a los intereses vitales del interesado, siendo ejemplos de esta situación los tratamientos que podrían ser necesarios en supuestos de control de epidemias y la su propagación o situaciones de emergencia humanitaria, en caso de catástrofes naturales o de origen humano, como serían los supuestos planteados en la consulta. Además, también se pone de manifiesto que la base jurídica del interés vital entra en juego sólo con carácter subsidiario, es decir, cuando no se cuenta con alguna otra de las bases previstas. Por tanto, aunque no se puede descartar que la protección del interés vital pueda actuar como base jurídica para el tratamiento que se pretende llevar a cabo, al menos en determinados casos, procede examinar antes si la base jurídica prevista en la letra e) puede habilitar el tratamiento.

La base jurídica prevista en la letra e) del artículo 6.1 del RGPD requiere, como ya se ha expuesto, de una norma con rango de ley que atribuya la misión en interés público o el poder público de que se trate. En el caso que nos ocupa, la Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local (LRBRL) dispone, en los artículos 25 y siguientes, que el municipio ejercerá, en todo caso, competencias en los términos de la legislación del Estado y de las Comunidades autónomas en determinadas materias, entre ellas: medio ambiente urbano y, en particular, parques y jardines públicos, gestión de los residuos sólidos urbanos y protección contra la contaminación acústica, lumínica y atmosférica en zonas urbanas (25.2.b), de policía local y protección civil y extinción de incendios (25.2.f), protección de la salubridad pública (25.2.j), que podrían comportar la actuación del municipio en supuestos como los expuestos en la consulta relativa a situaciones de alarma provocadas por epidemias o catástrofes de origen humano.

Más en concreto, la Ley 4/1997, de 20 de mayo, de protección civil de Cataluña, que tiene por objeto “la protección civil en Cataluña, que comprende las acciones destinadas a proteger a las personas, los bienes y el medio ambiente ante situaciones de grave riesgo colectivo, de catástrofes y de calamidades públicas”, reconoce a los alcaldes como autoridades de protección civil (artículo 40) ya los municipios como entidades básicas de la protección civil en Cataluña y con capacidad general de actuación y planificación en esta materia (artículo 47).

Asimismo, en materia de salud pública la Ley 18/2009, de 22 de octubre, de salud pública de Cataluña, considera a los ayuntamientos entes competentes en esta materia. El artículo 52 de esta norma enumera el conjunto de servicios mínimos en materia de salud pública que pueden prestar:

“a) La educación sanitaria en el ámbito de las competencias locales. b) La gestión del riesgo para la salud derivado de la contaminación del medio. c) La gestión del riesgo para la salud en lo que se refiere a las aguas de consumo público. d) La gestión del riesgo para la salud en los equipamientos públicos y en los lugares habitados, incluidas las piscinas. e) La gestión del riesgo para la salud en las actividades de tatuaje, micropigmentación y piercing. f) La gestión del riesgo para la salud derivado de los productos alimenticios en las actividades del comercio minorista, del servicio y la venta directa de alimentos preparados a los consumidores, como actividad principal o complementaria de un establecimiento, con reparto a domicilio o sin, de la producción de ámbito local y del transporte urbano. Se excluye la actividad de suministro de alimentos preparados para colectividades, otros establecimientos o puntos de venta. g) La gestión del riesgo para la salud derivado de los animales domésticos, animales de compañía, animales salvajes urbanos y plagas. h) La policía sanitaria mortuoria en el ámbito de las competencias locales. i) Las demás actividades de competencia de los ayuntamientos en materia de salud pública, de acuerdo con la legislación vigente en esta materia.”

Por tanto, se puede concluir que, de acuerdo con las normas con rango de ley mencionadas y otras que atribuyen competencias a los entes locales en materia de emergencias, el tratamiento de los datos para la comunicación a la población del municipio de situaciones de emergencia en el ámbito de las competencias municipales, puede considerarse necesario para el ejercicio de una misión en interés público o de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e) RGPD). Por tanto, ésta podría constituir la base jurídica del tratamiento.

## V

Ahora bien, de acuerdo con el RGPD todo tratamiento de datos, además de ser lícito, debe cumplir el resto de principios y garantías que establece el propio Reglamento, entre los que hay que tener en consideración, a los efectos que nos ocupan, el principio de limitación de la finalidad del tratamiento (artículo 5.1.b) RGPD), según el cual los datos se deben tratar de modo lícito y legítimos, y no serán tratados ulteriormente de modo incompatible con dichas fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórico o fines estadísticos no se considerará incompatible con los fines iniciales”.

La utilización de los datos personales que el Ayuntamiento dispone para la identificación de las llamadas recibidas en el sistema de atención emergencias 092 de la Guardia Urbana, para una finalidad ulterior distinta, como podría ser la comunicación a los titulares de los teléfonos de posibles situaciones emergencia, sería un tratamiento de datos que, en principio, podría entrar en conflicto con el principio de limitación de la finalidad.

En este sentido, el artículo 6.4 del RGPD prevé que:

“Cuando el tratamiento para otro fin distinto del 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, al objeto de determinar si el tratamiento con otro fin es compatible con el fin para el que se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

- a) cualquier relación entre los fines para los que se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
- b) el contexto en el 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.”

Por tanto, de acuerdo con el RGPD el tratamiento de datos para una finalidad diferente a la que se recogieron se puede fundamentar o bien en el consentimiento de los interesados, o en el derecho de la Unión o de los Estados miembros que constituya una medida para la salvaguarda de los objetivos indicados en el artículo 23.1, o bien superar el análisis de compatibilidad de acuerdo con los criterios enumerados.

Obviamente no habría problema para el cambio de fin si se contara con el consentimiento de las personas afectadas. Ahora bien, más allá de esto, en el caso que nos ocupa, las finalidades para las que se quieren utilizar los datos estarían alineadas con los objetivos de seguridad pública, de protección del interesado o de los derechos de otras personas, u otros objetivos de interés público a que se refiere el artículo 23.1 RGPD, por lo que es preciso ver si existe alguna norma con rango de ley que permita el cambio de finalidad.

La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (en adelante LGT), regula en su artículo 49 las guías de abonados y establece en su apartado primero que:

La elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información sobre ellos se realizará en régimen de libre competencia.

A tal efecto, las empresas que asignen números de teléfono a los abonados deberán dar curso a todas las solicitudes razonables de suministro de información pertinente para la prestación de los servicios de información sobre números de abonados y guías accesibles al público, en un formato aprobado y en unas condiciones equitativas, objetivas, orientadas en función de las costas y no discriminatorias, estando sometido el suministro de la citada información y su posterior utilización a la normativa en materia de protección de datos vigente en cada momento.

El Ministerio de Industria, Energía y Turismo deberá suministrar gratuitamente a las entidades que vayan a elaborar guías telefónicas de abonados, a las que presten el servicio de consulta telefónica sobre números de abonado ya las que presten los servicios de llamadas de emergencia, los datos que le faciliten las operadoras, de conformidad con las condiciones que se establezcan mediante real decreto.”

Asimismo, la LGT prevé en su artículo 28.4 lo siguiente:

“4. En cualquier caso, la obligación de encaminar las llamadas a los servicios de emergencia sin derecho a contraprestación económica de ningún tipo debe ser asumida tanto por los operadoras que prestan servicios de comunicaciones electrónicas al público para efectuar llamadas nacionales a números de un plan nacional de numeración telefónica, como por los que explotan redes públicas de comunicaciones electrónicas. Esta obligación se impone a dichos operadoras respecto de las llamadas dirigidas al número telefónico 112 de atención a emergencias ya otros que se determinen mediante real decreto, incluidas aquellas que se efectúen desde teléfonos públicos de pago, sin que sea necesario utilizar ninguna forma de pago en estos casos.

En todo caso, el servicio de llamadas de emergencia será gratuito para los usuarios, cualquiera que sea la Administración pública responsable de su prestación y con independencia del tipo de terminal que se utilice.

Asimismo, los operadoras pondrán gratuitamente a disposición de las autoridades receptoras de dichas llamadas la información que mediante real decreto se determine relativa a la ubicación de su procedencia.”

El 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, desarrolla las condiciones de entrega de los datos a que se refieren los citados artículos de la LGT.

Así, el artículo 68 de este Real Decreto 424/2005 establece:

“(…)

**2. La Comisión del Mercado de las Telecomunicaciones deberá suministrar gratuitamente a las entidades que vayan a elaborar guías telefónicas de abonados, a las que presten el servicio de consulta telefónica sobre números de abonado ya las que presten los servicios de llamadas de emergencia. que le faciliten los operadoras, de conformidad con lo establecido en este reglamento, con las instrucciones que, en su caso, dicte la Comisión del Mercado de las Telecomunicaciones y con lo que a tal efecto se establezca por orden ministerial.**

Las datos referentes a los abonados que hubieran ejercido su derecho a no figurar en las guías accesibles al público únicamente se proporcionarán a las entidades titulares del servicio de atención de llamadas de emergencia. A estos efectos, se entenderá que los servicios de llamadas de emergencia son los prestados a través del número 112 y aquellos otros que determine la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

El suministro se realizará a solicitud expresa de la entidad interesada y previa resolución motivada de la Comisión del Mercado de las Telecomunicaciones, previo informe de la Agencia Española de Protección de Datos, en la que se reconozca que la entidad reúne los requisitos para acceder a los datos y se establezcan las condiciones de suministro y de utilización de las datos suministrados.

**3. Las entidades que reciban las datos de la Comisión del Mercado de las Telecomunicaciones estarán obligadas a la prestación de los servicios que motiven la comunicación de las datos, a la utilización de las datos comunicadas única y exclusivamente para dicha prestación ya la utilización para ello de la última versión actualizada de las datos que se encuentre disponible.**

En caso de que en el plazo de seis meses desde el reconocimiento del derecho de la entidad solicitante al acceso a las datos del abonado ésta no hubiese iniciado la prestación de los servicios en virtud de los cuales se acordó el suministro de la información, o se comprobare que con posterioridad al reconocimiento del derecho los datos se utilizan para otras finalidades distintas o son empleadas de forma distinta a la establecida por la Comisión del Mercado de las Telecomunicaciones, ésta, previo informe de la Agencia Española de Protección de Datos, dictará resolución motivada que revoque, en su caso, la resolución por la que se reconozca el derecho de acceso a los datos.

Si se acordara la revocación de la resolución por la que se reconoció el derecho de acceso a los datos, la entidad interesada deberá proceder a la supresión inmediata de los datos que le hubieran sido comunicados, así como cualquier copia de los mismos.

Lo establecido en este apartado se entiende sin perjuicio de las competencias atribuidas a la Agencia Española de Protección de Datos por la legislación vigente en materia de protección de datos de carácter personal.”

Este Real Decreto está desarrollado por la “Circular 1/2013, relativa al procedimiento de suministro de datos de los abonados para la prestación de servicios de guías, consulta telefónica sobre números de abonado y emergencia” (modificada por la Circular 1/2014), en la



que, entre otras cuestiones, se identifican las entidades con derecho al suministro de los datos de los abonados contenidos en la base de datos (SGDA) y el procedimiento para su solicitud.

En principio la normativa de telecomunicaciones analizada no contempla la posibilidad de utilizar los datos de los abonados contenidos en la base de datos SGDA para otros fines distintos a la de elaborar las guías telefónicas de los abonados, la prestación del servicio de consulta telefónica sobre números de abonados y la prestación de servicios de llamadas de emergencia.

Por tanto, a falta de una norma con rango de ley que habilite el tratamiento, el ayuntamiento debería efectuar un análisis de la compatibilidad del tratamiento aplicando los criterios establecidos por el artículo 6.4 del RGPD

En este análisis se debe valorar, en primer lugar, la relación entre las finalidades para las que se hayan recogido los datos personales y las finalidades del tratamiento ulterior previsto. En caso de que nos ocupe la finalidad del tratamiento de los datos por el sistema de emergencias para la localización de la persona que comunica una emergencia y la realización de las gestiones necesarias para prestar el servicio, podrían tener una cierta relación con la finalidad de ponerse en contacto con los abonados para comunicar situaciones de emergencia o dirigirles recomendaciones en casos como los planteados en la consulta, puesto que en ambos casos se trata de la prestación de servicios a los ciudadanos en situaciones de emergencia.

Sin embargo, hay que tener en cuenta las limitaciones que la propia normativa impone a la utilización de estos datos con otros fines. En concreto, es necesario tener en cuenta el apartado 3 del artículo 68 del Real Decreto 424/2005.:

La normativa de telecomunicaciones mencionada establece, pues, un régimen tasado de comunicación de los datos de los abonados para su utilización por las entidades que tienen encomendadas la gestión del servicio de llamadas de emergencias al 112 -u otros equivalentes que se hayan establecido-, como sería el caso del 092- que excluye la utilización de los datos para una finalidad ulterior distinta.

En este sentido la Resolución de 15 de septiembre de 2009 de la Comisión del Mercado de las Telecomunicaciones, que se adjunta a la consulta, establece las condiciones de la cesión de los datos y contempla expresamente que la información será tratada única y exclusivamente para la finalidad para la que fue entregada, que los datos de los abonados se actualizarán de acuerdo con la circular de actualización, que los servicios serán prestados conforme a las características y condiciones que su normativa específica regula y que se garantizará el respeto a la legislación de protección de datos.

Por otra parte, es necesario tener en consideración la modificación del artículo 155 de la Ley 40/2015, de 1 de octubre de régimen jurídico del sector público, introducida por el Real Decreto 14/2019 de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Este artículo establece, en relación con la comunicación de datos entre administraciones

1. De conformidad con 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 personales y a la libre circulación de estos

datos y por lo que se deroga la Directiva 95/46/CE y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a las datos relativas a los interesados que obran en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichas datos con las máximas garantías de seguridad, integridad y disponibilidad.

2. En ningún caso podrá procederse a un tratamiento ulterior de los datos para fines incompatibles con el fin para el que se recogieron inicialmente los datos personales. De acuerdo con lo previsto en el artículo 5.1.b) del Reglamento (UE) 2016/679, no se considerará incompatible con los fines iniciales el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

3. Fuera del caso previsto en el apartado anterior y siempre que las leyes especiales aplicables a los respectivos tratamientos no prohíban expresamente el tratamiento ulterior de los datos para una finalidad distinta, cuando la Administración Pública cesionaria de los datos pretenda el tratamiento ulterior de los mismos para una finalidad que estime compatible con el fin inicial, deberá comunicarlo previamente a la Administración Pública cedente a efectos de que ésta pueda comprobar dicha compatibilidad. La Administración Pública cedente podrá, en el plazo de diez días oponerse motivadamente. Cuando la Administración cedente sea la Administración General del Estado podrá en este supuesto, excepcionalmente y de forma motivada, suspender la transmisión de datos por razones de seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación. En tanto que la Administración Pública cedente no comunique su decisión a la cesionaria ésta no podrá emplear las d

Se exceptúan de lo dispuesto en el párrafo anterior los supuestos en que el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales esté previsto en una norma con rango de ley de conformidad con lo previsto en el artículo 23.1 del Reglamento (UE) 2016/679.»

En definitiva, en aquellos casos en que la administración pública cesionaria de los datos, considere que la finalidad ulterior es compatible con la finalidad para la que se cedieron los datos, supuesto que, por la información disponible, no parece que concurra en el caso que nos ocupa, antes de efectuar el tratamiento, deberá comunicarlo a la administración cedente para que ésta verifique esta compatibilidad, con la posibilidad de oponerse a este cambio de finalidad.

Por tanto, se puede concluir, en cuanto a las tres primeras cuestiones planteadas en la consulta que, a pesar de que los supuestos previstos en las letras e) y d) del artículo 6 RGPD pueden constituir una base legítima del tratamiento, el principio de limitación de la finalidad impediría al ayuntamiento el tratamiento de los datos de la base de datos del Sistema de gestión de datos de abonados (SGDA) facilitada por la CNMT para gestionar las llamadas al teléfono 112, para una finalidad ulterior distinta como sería efectuar avisos a la población en casos de e

## VI

En la consulta también se plantea si “¿Sería necesario habilitar una aplicación móvil o web para que los ciudadanos se dieran de alta?”

De la normativa de protección de datos no se deriva la necesidad de habilitar una app o espacio en la web para que los ciudadanos puedan darse de alta. Ahora bien, el consentimiento puede ser una de las bases jurídicas en las que se fundamente el tratamiento.

El consentimiento como base legítima del tratamiento debe cumplir los requisitos establecidos en el artículo 4, apartado 11, del RGPD que define el consentimiento como: “cualquier indicación libre, específica, informada e inequívoca de la voluntad del interesado por la que, mediante declaración o acción afirmativa clara, signifique un acuerdo para el tratamiento de las datos personales relacionados con él”.

En el caso de las administraciones públicas el considerante 43 del RGPD dice: “Para garantizar que el consentimiento se concede libremente, el consentimiento no debe constituir un motivo jurídico válido para el tratamiento de datos personales en un caso específico en que exista un claro desequilibrio entre el interesado y el responsable del tratamiento, en particular cuando el responsable del tratamiento es una autoridad pública y, por tanto, es poco probable que el consentimiento se haya dado libremente en todas las circunstancias de esa situación específica. (... )”

En el análisis sobre el consentimiento efectuado por las Directrices 5/2020 sobre el consentimiento en el Reglamento 2016/679, del Comité Europeo de Protección de Datos, adoptado el pasado 4 de mayo de 2020, se hace mención a que “es poco probable que las autoridades públicas puedan confiar en el consentimiento para el tratamiento, puesto que cuando el responsable es una autoridad pública, a menudo existe un claro desequilibrio de poder en la relación entre el responsable y el interesado. También está claro en la mayoría de los casos que el interesado no tendrá alternativas realistas a aceptar el tratamiento (términos) de este controlador” (pá

Sin embargo, el Consejo pone de manifiesto que, “el uso del consentimiento como base legal para el tratamiento de datos por parte de las autoridades públicas no queda totalmente excluido en el marco jurídico del RGPD” y muestra algunos ejemplos de tratamientos de datos efectuados por administraciones públicas que tienen como base jurídica el consentimiento. En estos ejemplos se pone el énfasis en la capacidad del ciudadano de decidir sobre sus datos de tal modo que en caso de no dar el consentimiento esto no le comporte un perjuicio ni el privio de ningún servicio básico de la entidad pública, ni el ejercicio de ningún derecho.

Por tanto, si el ayuntamiento opta por un sistema basado en una aplicación móvil o web que permita la recogida del consentimiento informado de los interesados para el tratamiento de sus datos, para que el consentimiento constituya una base legítima del tratamiento, el ciudadano ha tener la posibilidad de denegar este consentimiento o simplemente no hacer uso de este sistema sin que esto le comporte un perjuicio o el privio de ningún servicio básico. En consecuencia, el ayuntamiento deberá habilitar otros canales que garanticen la comunicación con la población en estas situaciones de emergencia, como podría ser, por ejemplo, la comunicación a través de los medios c

comunicación, a través de la web municipal, mediante avisos por megafonía a toda la población, etc.

En la implementación de una aplicación móvil o web en la que los ciudadanos se den de alta, el ayuntamiento debe tener en consideración los principios de privacidad desde el diseño y por defecto, así como el de responsabilidad proactiva para garantizar que ésta cumple con las previsiones del RGPD y LOPDGDD.

## VII

Finalmente, en cuanto a la cuestión relativa a la transposición del Código Europeo de Comunicaciones electrónicas y la posibilidad de utilizar este mecanismo únicamente por los ciudadanos del municipio, se realizan las siguientes consideraciones.

El Código Europeo de Comunicaciones Electrónicas, aprobado por la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, obliga a los Estados miembros a utilizar, un sistema 112 inverso para advertir a la población en situaciones de emergencia enviando alertas a los posibles afectados a través de las redes telefónicas y fija como plazo de transposición de esta medida el 21 de junio de 2022. Así, el artículo 110 de esta norma prevé:

### “Sistema de alerta público

1. A más tardar el 21 de junio de 2022, cuando existan sistemas de alerta público en caso de grandes catástrofes o emergencias inminentes o en curso, los Estados miembros velarán por que los proveedores de servicios móviles de comunicaciones interpersonales basados en numeración transmiten las alertas a los usuarios finales afectados.

2. No obstante lo estipulado en el apartado 1, los Estados miembros podrán establecer que las alertas se transmitan mediante servicios de comunicaciones electrónicas disponibles al público distintos de los indicados en el apartado 1 y distintos otros servicios de radiodifusión, o mediante de una aplicación móvil basada en un servicio de acceso a través de internet, siempre que la eficacia del sistema de alerta sea equivalente en términos de cobertura y capacidad para abarcar a los usuarios finales, incluso aquellos que se encuentren de forma temporal en el área en cuestión, teniendo muy presentes las indicaciones del ORECE. Los usuarios finales tendrán que poder recibir las alertas fácilmente.

A más tardar el 21 de junio de 2020 y tras consultar con las autoridades a cargo de los PSAP, el ORECE publicará directrices sobre la forma de evaluar si la efectividad de los sistemas de alerta público previstos en el presente apartado es equivalente a la efectividad de los previstos en el apartado 1.”

Sin perjuicio de que la norma que transponga esta Directiva podría dar cobertura al tratamiento que se pretende llevar a cabo, no parece que en el momento actual, en el que todavía no ha transcurrido el plazo para su transposición, concurren los requisitos necesarios para que esta norma pueda tener efecto directo.

Por tanto, tal y como se ha expuesto en el fundamento jurídico precedente, desde el punto de vista de la normativa de protección de datos y en relación con la consulta concreta planteada, el ayuntamiento, en el ámbito de sus competencias únicamente podría implementar y utilizar un sistema de comunicación de alarmas en la población de su municipio, con el consentimiento de los interesados recogido mediante un sistema que ofrezca todas las garantías en lo que respecta a la gestión de los datos de acuerdo con el RGPD.

### Conclusiones

El principio de limitación de la finalidad del RGPD impediría al ayuntamiento utilizar los datos de la base de datos del Sistema de gestión de datos de abonados (SGDA) facilitada por la CNMT para una finalidad ulterior distinta como sería efectuar avisos a la población en casos de emergencias graves.

El consentimiento de los interesados recogido en una aplicación móvil o web podría ser una base legítima de ese tratamiento.

Barcelona 4 de junio de 2020

Traducción Automática