N/REF: 424190/2016

Se consulta si resulta conforme a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la publicación de los datos de los habitantes de una determinada población, sin que se incluya el nombre y DNI, relativos a fecha de nacimiento, nacionalidad, nivel de estudios y calle sin identificar ni portal ni número, con la finalidad de que se desarrollen aplicaciones software por terceros o el propio Ayuntamiento que crucen datos del portal Opendata que sean de interés para el ciudadano.

Con carácter general, debe indicarse que los artículos 1 y 2 de la Ley Orgánica 15/1999, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la citada Ley como "cualquier información concerniente a personas físicas identificadas o identificables."

El artículo 5.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, concreta la definición de dato personal especificando que constituye un dato de carácter personal *"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables."*

Por otra parte, la definición contenida en el artículo 3.a de la Ley Orgánica 15/1999 se complementa con la de persona identificable, a la que se refiere el artículo 5.1.o) de su Reglamento de desarrollo, que dispone que lo será *"toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados".*

Ambas definiciones tienen su origen en lo establecido en la Directiva 95/46/CE, cuyo artículo 3 califica como dato personal "*toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o*

varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Para determinar que se entiende por persona identificada o identificable, cabe acudir a lo señalado, en el Dictamen 4/2007 del Grupo de Trabajo del artículo 29, órgano consultivo independiente de la Unión Europea sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Dicho dictamen analiza los términos contenidos en la definición aportada por la Directiva señalando respecto al concepto de persona identificada o identificable lo siguiente:

> "La Directiva requiere que la información se refiera a una persona física «identificada o identificable». Ello suscita las siguientes consideraciones. De modo general, se puede considerar «identificada» a una persona física cuando, dentro de un grupo de personas, se la «distingue» de todos los demás miembros del grupo. Por consiguiente, la persona física es «identificable» cuando, aunque no se la haya identificado todavía, sea posible hacerlo (que es el significado del sufijo «ble»). Así pues, esta segunda alternativa es, en la práctica, la condición suficiente para considerar que la información entra en el ámbito de aplicación del tercer componente. La identificación se logra normalmente a través de datos concretos que podemos llamar «identificadores» y que tienen una relación privilegiada y muy cercana con una determinada persona. Cabe citar como ejemplos su apariencia exterior, es decir su altura, el color del cabello, la ropa, etc. o una cualidad de la persona que no puede percibirse inmediatamente, como su profesión, el cargo que ocupa, su nombre, etc. La Directiva menciona esos «identificadores» en la definición de «datos personales» del artículo 2 cuando establece que «se declarará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

En lo que respecta a los términos "directa" o "indirectamente" identificable continúa señalando el Grupo de Trabajo del artículo 29 que:

> "Esta idea se aclara aún más en los comentarios a los artículos de la propuesta modificada de la Comisión, en donde se afirma que «una

persona puede ser identificada directamente por su nombre y apellidos o indirectamente por un número de teléfono, la matrícula de un coche, un número de seguridad social, un número de pasaporte o por una combinación de criterios significativos (edad, empleo, domicilio, etc.), que haga posible su identificación al estrecharse el grupo al que pertenece."

Los términos de esta declaración indican claramente que el que determinados identificadores se consideren suficientes para lograr la identificación es algo que depende del contexto de la situación de que se trate. Un apellido muy común no bastará para identificar a una persona - es decir, para aislarla – dentro del conjunto de la población de un país, mientras que es probable que permita la identificación de un alumno dentro de una clase. Incluso una información auxiliar, como, por ejemplo, «el hombre que lleva un traje negro», puede identificar a alguno de los transeúntes que esperan en un semáforo. Así pues, el que se identifique o no a la persona a la que se refiere una información depende de las circunstancias concretas del caso.

Por su parte, cuando hablamos de «indirectamente» identificadas o identificables, nos estamos refiriendo en general al fenómeno de las «combinaciones únicas», sean éstas pequeñas o grandes. En los casos en que, a primera vista, los identificadores disponibles no permiten singularizar a una persona determinada, ésta aún puede ser «identificable», porque esa información combinada con otros datos (tanto si el responsable de su tratamiento tiene conocimiento de ellos como si no) permitirá distinguir a esa persona de otras. Aquí es donde la Directiva se refiere a «uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social». Algunas de esas características son tan únicas que permiten identificar a una persona sin esfuerzo (el «actual Presidente del Gobierno de España »), pero una combinación de detalles pertenecientes a distintas categorías (edad, origen regional, etc.) también puede ser lo bastante concluyente en algunas circunstancias, en especial si se tiene acceso a información adicional de determinado tipo. Este fenómeno ha sido estudiado ampliamente por los estadísticos, siempre dispuestos a evitar cualquier quebrantamiento de la confidencialidad."

Estas definiciones deben ponerse en relación con lo que se viene denominando "datos abiertos" a fin de delimitar en qué supuestos y con qué condiciones pueden los datos personales obrantes en los archivos de las

Administraciones públicas considerarse como datos abiertos o susceptibles de reutilización

En este sentido, la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público, planteaba como objetivo que la información del sector público que estuviese a disposición del público con arreglo a la legislación nacional pudiera ser reutilizada con fines comerciales o no comerciales. Desde el punto de vista de la normativa de protección de datos, el considerando 21 de la mencionada Directiva 2003/98/CE dispone que "La presente Directiva se debe incorporar al Derecho interno y aplicar de forma que se cumplan plenamente los principios relativos a la protección de los datos personales, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos".

Este principio se reitera en la reforma operada por la Directiva 2013/37/UE, del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE, cuyo considerando 34 señala que "La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea, incluidos la protección de los datos de carácter personal (artículo 8) y el derecho a la propiedad (artículo 17). Nada de lo contenido en la presente Directiva debe interpretarse o aplicarse en un sentido que no sea acorde con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales". En particular, en lo que al derecho fundamental a la protección de datos se refiere, el considerando 11 de la Directiva añade, con mayor precisión que la contenida en la Primera Directiva, que "la presente Directiva debe incorporarse al Derecho interno y aplicarse de forma que se cumplan plenamente los principios relativos a la protección de los datos personales, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En particular, conviene señalar que, con arreglo a dicha Directiva, los Estados miembros deben determinar las condiciones en las que sea legal el tratamiento de datos personales. Además, uno de los principios de dicha Directiva consiste en que los datos personales no deben ser tratados posteriormente a una recogida de

un modo que sea incompatible con los objetivos determinados, explícitos y legítimos para los que dichos datos fueron recogidos".

El texto actualmente vigente de la Directiva 2003/98 incide aún en mayor medida en el necesario respeto a las normas de protección de datos, por cuanto el nuevo artículo 1.2 c quater excluye del ámbito de aplicación de la misma:

"-Los documentos a los que no pueda accederse en virtud de regímenes de acceso por motivos de protección de los datos personales.

-Los documentos cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de los datos personales.

- Las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales."

Respecto de las limitaciones a la reutilización derivadas de este precepto, debe tenerse en cuenta lo señalado por el aludido Grupo de Trabajo del artículo 29 en su Dictamen 06/2013 sobre datos abiertos y reutilización de la información del sector público (ISP), adoptado el 5 de junio de 2013, en que, como primera conclusión, se pone de manifiesto que "el «principio de reutilización» no es automático cuando está en juego el derecho a la protección de los datos personales, y no anula las disposiciones aplicables de la normativa sobre protección de datos. Cuando los documentos en poder de los organismos del sector público contienen datos personales, su reutilización está incluida en el ámbito de aplicación de la Directiva 95/46/CE y, por tanto, está sujeta a la normativa sobre protección de datos aplicable", añadiendo así que "en los casos en que la reutilización incluye datos personales, el organismo del sector público no puede invocar sistemáticamente la necesidad de cumplir con la Directiva ISP como razón legítima para facilitar datos para su reutilización", de modo que que, "desde la perspectiva de quien reutiliza los datos, la Directiva ISP en sí misma no crea un motivo legítimo para el tratamiento".

A continuación, el apartado V del Dictamen se dedica específicamente al análisis de las limitaciones al principio de reutilización vinculadas a la aplicación de las normas reguladoras del derecho fundamental a la protección de datos de carácter personal, que resultan especialmente de interés en tanto que el

artículo 3.j de la Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público reproduce lo establecido en la el artículo 1.2.c) quater de la Directiva 2003/98. Dispone el aludido artículo 3.j " La presente Ley no será aplicable a los siguientes documentos que obren en las Administraciones y organismos del sector público previstos en el artículo 2: (…) j) Los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de los datos personales, de conformidad con la normativa vigente y las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales."

El Dictamen diferencia tres límites a la reutilización derivados de la aplicación de las normas de protección de datos, vinculados a su vez con lo establecido en los distintos Estados Miembros en relación con el acceso a la información del sector público:

El primer supuesto se refiere a los supuestos en que está prohibido el acceso en aplicación de las normas de protección de datos de carácter personal, recordando la doctrina establecida por el Tribunal de Justicia de la Unión en diversas sentencias y vinculando esta prohibición general a lo dispuesto en la normativa de los distintos Estados Miembros en relación con el acceso a la información pública. Así, se hace referencia a las sentencias del TJ de 20 de mayo de 2003 (Asunto Österreichischer Rundfunk) y de 9 de noviembre de 2010 (Asunto Volker und Markus Schecke), que coinciden en establecer que el mero acceso a la información pública, como restricción a un derecho fundamental, el de protección de datos de carácter personal, debe cumplir los requisitos exigidos para ello por el Convenio Europeo de Derechos Humanos y la jurisprudencia del Tribunal Europeo de Derechos Humanos; es decir, estar prevista en una Ley, perseguir un objetivo legítimo y constituir una medida proporcional en una sociedad democrática para obtener ese objetivo. En el mismo sentido, cabe hacer referencia a la Sentencia de 29 de junio de 2010 (asunto Bavarian Lager).

Una segunda categoría de supuestos, según el Dictamen, incluiría aquellos documentos cuyo acceso esté limitado como consecuencia de la aplicación de las normas de protección de datos, que imponen alguna exigencia adicional para el acceso, como por ejemplo la acreditación de un interés legítimo por parte del solicitante, tal y como ocurriría, por ejemplo, en

España para el acceso al Registro de la Propiedad, en los términos establecidos en la Ley Hipotecaria, que exige la concurrencia del mencionado interés en el solicitante de la publicidad registral.

Por último, el Dictamen se refiere a una tercera categoría de documentos del sector público en que el régimen aplicable puede resultar más complejo, cuales son aquéllos que en principio pueden ser susceptibles de acceso conforme a la normativa de acceso a la información pública, pero cuya reutilización se encuentra limitada por resultar incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales. A tal efecto, el Dictamen se refiere a una serie de ejemplos que pudieran ser aplicables y concluye lo siguiente:

> "En todos los casos, el organismo del sector público interesado debe realizar una cuidadosa evaluación de impacto sobre la protección de datos para decidir si pueden facilitarse los datos para su reutilización en la Directiva ISP y, de ser así, si la legislación sobre protección de datos requiere condiciones específicas y salvaguardias. El «principio de reutilización» no es automático, y no puede tener prioridad sobre las disposiciones aplicables de la normativa de protección de datos.
>
> Esta evaluación detallada es tanto más importante dado que, en virtud de la Directiva ISP, el organismo del sector público, en principio, no debe analizar quién es el solicitante concreto que pide acceso para la reutilización. De conformidad con el artículo 10 (No discriminación), «las condiciones que se apliquen para la reutilización de un documento no deberán ser discriminatorias para categorías comparables de reutilización». Asimismo, conformidad con el artículo 11 (Prohibición de los acuerdos exclusivos), «la reutilización de documentos estará abierta a todos los agentes potenciales del mercado... Los contratos o acuerdos de otro tipo entre los organismos del sector público que conserven los documentos y los terceros no otorgarán derechos exclusivos.»
>
> Por consiguiente, al decidir si autorizan o no la reutilización, los organismos del sector público deben tener en cuenta la compatibilidad de permitir la reutilización en virtud de una licencia abierta no solo al solicitante, sino también a cualquiera que pida los datos. Esto requiere un alto nivel de confianza en que ninguno de los reutilizadores potenciales podrá hacer un uso indebido de los datos personales facilitados.

> La Directiva ISP no excluye que los términos y condiciones puedan autorizar el tratamiento solo para fines específicos. La cuestión que se plantea al organismo del sector público es por tanto si la reutilización, por cualquier «posible agente del mercado», a estos efectos, es compatible con las finalidades previstas por el organismo del sector público. La potencial reutilización por parte de las entidades financieras de la información sobre el pago de impuestos, por ejemplo, para fines de información crediticia, es pertinente ya que siguen siendo un potencial reutilizador, según el criterio de «cualquier persona». Por tanto, para resolver los problemas de protección de datos y en particular para garantizar el cumplimiento del principio de limitación de la finalidad, el organismo del sector público (o el legislador) deberá poder limitar, en su caso, las finalidades de la reutilización."

En el presente proyecto se hace referencia a la publicación de determinados datos contenidos en el Padrón municipal del Ayuntamiento consultante, cuyo régimen quedaría incluido en aquéllos a que hace referencia el artículo 3.j de la Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, por lo que no puede considerarse que los datos contenidos en el mismo son susceptibles de reutilización, de este modo será preciso que cualquier comunicación de los datos personales en él contenidos sea conforme a lo establecido en la Ley Orgánica 15/1999.

Debe así tenerse en cuenta que ley Orgánica 15/1999 califica como una cesión de datos a "*toda revelación de datos realizada a una persona distinta del interesado",* por lo que la publicación de datos personales contenidos en el fichero a que hace referencia la consulta vendría a constituir una cesión de datos. Dicha cesión debe someterse al régimen general previsto para las comunicaciones de datos en el artículo 11 de la misma Ley, donde se establece que la misma solo puede verificarse para el cumplimiento de fines directamente relacionados con las funciones legitimas del cedente y cesionario y exige, para que pueda tener lugar, el consentimiento del interesado (artículo 11.1), otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar (artículo 11.3), y que debe recabar el cedente como responsable del fichero que contiene los datos que se pretenden ceder. El número segundo de dicho artículo recoge un conjunto de excepciones a la necesidad de consentimiento del interesado que no son de aplicación al presente caso.

No obstante, no resulta aplicable la normativa de protección de datos cuando no sea posible identificar a las personas, por haberse sometido sus datos a un proceso de disociación; la Ley Orgánica 15/1999 describe éste en su artículo 3 f) como "*Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable"* Debe a este respecto tomarse en consideración lo indicado por el grupo de Trabajo del artículo 29 en el aludido Dictamen 6/2013 en cuanto a la posibilidad de facilitar datos contenidos en los ficheros de las Administraciones Públicas eliminando datos personales, que a continuación se reproduce parcialmente:

> "Hasta la fecha, las iniciativas sobre reutilización de la ISP lanzadas por los organismos del sector público a través de «portales de datos abiertos» u otras plataformas han tenido generalmente como objetivo facilitar datos agregados y anonimizados para su reutilización, en vez de datos personales como tales. Este planteamiento es más seguro y debe fomentarse.
>
> Las leyes de protección de datos no suelen permitir que los organismos del sector público publiquen datos personales recogidos para otro fin, generalmente administrativo. Por tanto, en estos casos, su reutilización como parte de las iniciativas de reutilización de la ISP tampoco es posible. En vez de datos personales, se facilitan y deberían facilitarse (en principio) datos estadísticos derivados de los datos personales. Esta es la solución más eficaz para minimizar el riesgo de revelación inadvertida de datos personales. Estas series de datos agregados y anonimizados no deberán permitir la reidentificación de las personas y, por tanto, no deben contener datos personales.
>
> Decidir el nivel de agregación adecuado y las técnicas específicas de anonimización que deben utilizarse es una tarea difícil. Si la agregación y la anonimización no se hacen de manera eficaz, esto entraña el riesgo de que los individuos puedan ser reidentificados a partir de estos conjuntos de datos. Por tanto, la legislación sobre protección de datos tiene un papel importante que desempeñar a la hora de contribuir a determinar el umbral a partir del cual es «seguro» comunicar datos agregados y anonimizados como parte de una iniciativa de la ISP.
>
> La Directiva 95/46/CE establece un alto nivel para el umbral de anonimización. En el presente documento, el término «anonimización» se

refiere a los datos que ya no pueden considerarse datos personales de conformidad con el artículo 2, letra a), de la Directiva 95/46/CE. El artículo 2, apartado a) define los «datos personales» como «toda información sobre una persona física identificada o identificable (el "interesado")». Se considerará identificable «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social»

.

El considerando 26 de la Directiva 95/46/CE es también pertinente y dispone además que, con el fin de «determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona».

Hay que señalar que ello establece un umbral elevado, como se expondrá más adelante en el presente Dictamen. Salvo que los datos puedan anonimizarse para alcanzar este umbral, sigue siendo aplicable la legislación sobre protección de datos. Esto significa, entre otras cosas, que a menos que se alcance el umbral, la publicación de la información (y cualquier uso posterior) debe ser «compatible» con las finalidades iniciales de la recogida de datos con arreglo al artículo 6, apartado 1, letra b), de la Directiva 95/46/CE. Además, también deberá existir una base jurídica adecuada para el tratamiento en virtud del artículo 7, apartado 2, letras a) a f), de la Directiva 95/46/CE (por ejemplo, el consentimiento, o necesidad de cumplir la ley). En cambio, si los datos han sido anonimizados en el sentido del artículo 2, letra a), y del considerando 26 de la Directiva 95/46/CE, las normas sobre protección de datos dejarán de ser aplicables y los reutilizadores podrán reutilizar los datos sin estas limitaciones Una vez más, es preciso hacer hincapié en el hecho de que «datos anonimizados», según el presente Dictamen, son datos que ya no se consideran personales. Los datos anonimizados deben distinguirse, en particular, de los datos que han sido manipulados utilizando diversas técnicas para mitigar los riesgos de reidentificación de los individuos en cuestión, pero que no han alcanzado el umbral establecido en el artículo 2, letra a), y en el considerando 26 de la Directiva 95/46/CE24. En muchos supuestos, estas técnicas solo resultan adecuadas para una divulgación limitada a efectos de su reutilización por terceros, pero no para su plena divulgación y reutilización con licencia abierta.

Es también importante hacer hincapié en que una vez que los datos se publican para su reutilización, no habrá control alguno sobre quién puede acceder a ellos. La probabilidad de que «cualquier otra persona» tenga los medios y los utilice para reidentificar a los interesados aumentará considerablemente. Por tanto, y con independencia de la interpretación del considerando 26 en otros contextos, cuando se trata de facilitar datos para su reutilización en virtud de la Directiva ISP, el Grupo de trabajo del artículo 29 desea dejar absolutamente claro que debe tenerse el mayor cuidado en garantizar que los conjuntos de datos facilitados no incluyan datos que puedan ser reidentificados por medios que puedan ser razonablemente utilizados por cualquier persona, incluidos los reutilizadores potenciales, pero también por otras partes que puedan tener interés en obtener los datos, incluidos los servicios con funciones coercitivas.

La anonimización es cada vez más difícil de lograr con el avance de las modernas tecnologías informáticas y la disponibilidad de la información de forma ubicua. La reidentificación de las personas es cada vez más común y representa una amenaza en la actualidad. En la práctica, existe una importante zona gris, en la que el responsable del tratamiento de datos puede creer que un conjunto de datos está anonimizado, pero un tercero puede ser capaz de identificar al menos a algunas personas a partir de estos datos, por ejemplo, utilizando otros datos públicos o cualquier otra información de que disponga.

Uno de los principales factores de riesgo es el aumento de la cantidad de datos en línea y fuera de línea, tanto a disposición del público como en manos de organizaciones empresariales, que pueden utilizarse para trazar el perfil de las personas con fines de publicidad comportamental y para un abanico creciente de otros fines. Al cotejarse con la realidad de los «grandes datos» de que ya disponen estas organizaciones, la ISP derivada de los datos personales y facilitada para su reutilización podría aumentar la probabilidad de que los particulares puedan ser identificados o de que sus perfiles pueden verse enriquecidos, a menudo sin que las personas sean conscientes de que esté ocurriendo.”

De este modo sólo será posible la publicación de datos contenidos en los ficheros de la Administración pública, fuera de los supuestos permitidos por la Ley o en que exista un consentimiento de los afectados, si los datos se encuentran anonimizados. Resulta de especial interés en lo que respecta a la

disociación de los datos lo indicado por el Grupo de Trabajo del artículo 29 en su Dictamen 5/2014 sobre técnicas de anonimización, en el que se ponía de manifiesto que:

> "El Grupo de Trabajo examinó el concepto de «datos personales» en el Dictamen 4/2007 sobre datos personales, en el que se centra en los elementos componentes de la definición del artículo 2, letra a), de la Directiva 95/46/CE, entre ellos la referencia a una persona física «identificada o identificable». En este contexto, el Grupo de Trabajo llegó a la conclusión de que «los datos anonimizados serían, por tanto, datos anónimos que antes hacían referencia a una persona identificable, pero que ahora ya no admiten identificación».
>
> Por consiguiente, el Grupo de Trabajo ya ha aclarado que la Directiva propone la razonabilidad de los medios usados («el conjunto de los medios que puedan ser razonablemente utilizados») como criterio para evaluar si el tratamiento de anonimización es suficientemente sólido, es decir, si la identificación es «razonablemente» imposible. Afectan directamente a la identificabilidad el contexto y las circunstancias particulares de cada caso.
>
> (…) Una solución de anonimización eficaz impide a todos singularizar a una persona en un conjunto de datos, vincular dos registros en un conjunto de datos (o dos registros pertenecientes a conjuntos diferentes) e inferir cualquier tipo de información a partir de dicho conjunto. En definitiva, como norma general, no basta con eliminar los elementos que pueden servir para identificar directamente a una persona para garantizar que ya no se puede identificar al interesado. Con frecuencia habrá que tomar medidas adicionales para evitar dicha identificación, las cuales dependerán una vez más del contexto y de los fines del tratamiento de que van a ser objeto los datos."

Recuerda asimismo dicho Dictamen que "Es importante dejar claro que el concepto de «identificación» no conlleva únicamente la posibilidad de recuperar el nombre o la dirección de una persona, sino que incluye también la identificabilidad potencial por singularización, vinculabilidad o inferencia. Es más, a efectos legales es irrelevante la intención del responsable del tratamiento o del destinatario. Mientras los datos sean identificables, se aplica la legislación sobre protección de datos."

Estos aspectos deben tenerse en cuenta respecto de los tratamientos y cesiones de datos a realizar por el Ayuntamiento en relación con el concepto de open data, en particular respecto de los datos que en tal calidad pudiera publicar y que sean resultado de un proceso de disociación de los datos personales obrantes en los ficheros municipales (sea el Padrón o cualquier otro que contenga datos personales), recordando que no es suficiente con eliminar los elementos que identifican directamente a la persona (nombre, dirección) como ocurre en el presente supuesto, sino que es preciso una agregación suficiente de los datos para evitar la re-identificación de las personas cuyos datos, aunque separados de los que le identifican directamente, se hacen públicos.