



N/REF: 319042/2017

La consulta expone que un periodista solicitó de la Administración consultante detalle de todas y cada una de las incidencias ocurridas registradas en el Sistema de notificación de incidencias acuáticas (AQUATICUS) desde la creación del fichero. Dicha solicitud de información fue denegada sobre la base de que dicho fichero contiene datos que se refieren a la salud de los ciudadanos, ya que el citado fichero recoge individualizadamente las incidencias en piscinas u otras zonas de baño [traumatismos, etc.], así como su intervención, seguimiento y desenlace [asistencia sanitaria, traslado hospitalario, fallecimiento, etc.], siendo estos los pedidos expresamente por el particular, por lo que sobre la base del párrafo segundo del artículo 15.1 de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, se deniega el acceso a la información. El solicitante acudió al Consejo de Transparencia frente a la citada decisión. El Consejo de Transparencia concluye que el Ministerio debe proporcionar la información solicitada, a excepción del campo relativo a la "edad" del afectado ya que, dicho Consejo entiende que: *"la supresión entre la información solicitada del dato relativo a la edad del afectado permite compatibilizar el interés público en el acceso a la información -debe recordarse que se trata en parte de una cuestión de seguridad pública y, de prestación de los servicios públicos para garantizarla- con la protección de los datos de carácter personal de los afectados"*

En definitiva, la consulta consiste en que por la AEPD se diga *"si el cumplimiento del requerimiento del Consejo de Transparencia y Buen Gobierno, facilitando los datos solicitados para cada una de las incidencias notificadas al Sistema AQUATICUS puede vulnerar en algún modo la legislación vigente en materia de protección de datos de carácter personal"*.

I

Debe señalarse como punto de partida que la solicitud del parecer de esta Agencia es en relación con determinadas cesiones de datos que se



derivan de lo acordado en resolución del Consejo de Transparencia y Buen Gobierno por la que se acuerda el acceso a determinada información referida a los datos que constan en el denominado fichero AQUATICUS.

En este sentido, debe recordarse que el artículo 38 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas establece que “los actos de las Administraciones Públicas sujetos al Derecho Administrativo serán ejecutivos con arreglo a lo dispuesto en esta Ley”, añadiendo el artículo 39.1 que “los actos de las Administraciones Públicas sujetos al Derecho Administrativo se presumirán válidos y producirán efectos desde la fecha en que se dicten, salvo que en ellos se disponga otra cosa”.

De este modo, habiéndose dictado por el Consejo de Transparencia y Buen Gobierno, en el ejercicio de sus competencias, resolución por la que se estima la reclamación de acceso a la información pública presentada, dicha resolución surtirá plenos efectos a menos que hubiera sido objeto de recurso contencioso-administrativo, y en su caso, con solicitud de suspensión. Por ello, esta Agencia Española de Protección de Datos no puede entrar a valorar la procedencia de las cesiones acordadas por el citado Consejo, que se encontrarían amparadas en el principio de eficacia de los actos administrativos, siendo la regulación legal de dicho principio la norma con rango de Ley que otorgaría cobertura a las cesiones de datos que implique el acceso acordado. Así pues, corresponde a la jurisdicción contencioso-administrativa la revisión de dicho acto administrativo, y ante la cual podrán exponerse cualesquiera circunstancias que pudieran dar lugar a la nulidad o anulabilidad del acto administrativo recurrido.

II

No obstante lo anterior hay que recordar que el artículo 5.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD), 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 (LOPD) 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.”

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 el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD) establece en su considerando 26:

*Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. **Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.** Para determinar si existe una **probabilidad razonable** de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.*

Igualmente en su considerando 53 hace referencia a los tratamientos de datos de salud, refiriéndose explícitamente a los datos “para fines relacionados con la salud”:

Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia

sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional. El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos.

En definitiva, y a los meros efectos del establecimiento de la posibilidad de que sea posible la identificación de una persona con los datos que constan en el fichero AQUATICUS una vez retirado el dato de la edad de la persona, no parece imposible que sea identificable una persona física con el resto de los datos, habida cuenta de que, tal y como menciona la consultante, la baja prevalencia de determinados incidentes en determinados lugares (ciudades de baja población, en determinadas épocas del año etc.) podría dar lugar a que sin necesidad de un esfuerzo desproporcionado en tiempo, por medio del resto de datos desagregados pudiera llegarse a identificar a la persona física cuyos datos de salud constan en el incidente de dicho fichero (por ejemplo, a través de búsquedas en los periódicos en las provincias donde ocurrió el incidente).

III

El anterior criterio se plantea a efectos meramente hipotéticos, ya que como hemos mencionado en el apartado I de este Informe, los actos



administrativos son eficaces desde que se dictan, y la ley de transparencia no prevé un recurso frente a las resoluciones del Consejo de Buen Gobierno antes esta AEPD, por lo que cualquier decisión a este respecto habrá de provenir de la jurisdicción contencioso-administrativa.