CNS 26/2010

Dictamen en relación con la consulta planteada por la Administración Pública Autonómica acerca del tratamiento de los datos contenidos en el Catálogo de Datos y Documentos Electrónicos

Se presenta ante la Agencia Catalana de Protección de Datos un escrito en el que se solicita el parecer de la Agencia en relación con la gestión del Catálogo de Datos y Documentos Electrónicos (en adelante, el Catálogo) y con el derecho de los ciudadanos y ciudadanas a no aportar determinados datos que la Administración Pública ya posee.

En concreto, se pide el posicionamiento de la Agencia con respecto a si el acceso a determinada información a través de una herramienta tecnológica, la Plataforma de Integración y Colaboración Administrativa (en adelante, la PICA), para verificar de oficio los datos aportados por la persona interesada, constituye o no una cesión de datos a los efectos de la normativa de protección de datos.

La PICA es una solución tecnológica que permite, entre otras cosas, intercambiar documentos y datos que se encuentran en algún órgano de la Generalitat o de otras administraciones y entidades (en este caso a través del Consorcio AOC) y así poderlos incorporar al trámite administrativo propio sin tener que pedirlos a los ciudadanos (según información disponible en la página web de la AOC, www.aoc.cat).

(...)

Analizada la petición y la normativa vigente aplicable, y visto el informe de la Asesoría Jurídica, se emite el siguiente dictamen:

I

(...)

II

Para situar la cuestión objeto de consulta, es preciso recordar que el Decreto 56/2009, de 7 de abril, para el impulso y desarrollo de los medios electrónicos en la Administración de la Generalitat, creó el Catálogo. En concreto, el artículo 17.1 dispone que:

> *"El Catálogo de Datos y Documentos Electrónicos es la relación actualizada de datos y documentos que obran en poder de los entes previstos en la letra a) del artículo 2.1 y de otras administraciones e instituciones públicas, y que se pueden obtener por medios electrónicos, al objeto de hacer efectivo el derecho de los ciudadanos y ciudadanas a no aportarlos a un procedimiento concreto".*

Más recientemente, la Ley 29/2010, de 3 de agosto, sobre el uso de los medios electrónicos en el sector público de Cataluña, dispone en su artículo 21, en relación con el Catálogo, que:

> *"1. El **Catálogo** de datos y documentos interoperables en Cataluña es la herramienta con la que se dota al sector público de Cataluña para **hacer efectivo el derecho de los ciudadanos a no aportar los datos y los documentos que obran en poder de las Administraciones Públicas.***
>
> *2. Las entidades que conforman el sector público de Cataluña deben incluir en el Catálogo de datos y documentos interoperables en Cataluña la relación actualizada de datos y documentos que se pueden obtener por*

medios electrónicos y los mecanismos de seguridad para acceder a ellos garantizando la seguridad, la integridad y la protección plena de los datos de carácter personal.

3. El Catálogo de datos y documentos interoperables en Cataluña, que está gestionado por el Consorcio Administración Abierta Electrónica de Cataluña, es accesible a través de la sede electrónica de la entidad correspondiente con arreglo a lo que establece el artículo 11.

4. Cada entidad debe establecer los mecanismos por medio de los cuales sus empleados públicos acceden a los datos y a los documentos incluidos en el Catálogo de datos y documentos interoperables en Cataluña, de acuerdo con los requisitos que ha establecido quien ha incluido los datos en este Catálogo y es responsable de él".

Los accesos a la información del Catálogo se realizan a través de la PICA.Como se explica en la consulta, el procedimiento de acceso se lleva a cabo teniendo en cuenta diversas cuestiones, que la consulta concreta en los términos siguientes:

"a) Los datos y documentos se ponen a disposición de las Administraciones Públicas interesadas que los requieran en y para el ejercicio de sus competencias; b) La Administración cedente determina las condiciones de acceso de las administraciones cesionarias; c) Ninguna Administración puede acceder a los datos de forma genérica; siempre hace falta una autorización previa para cada finalidad que justifique la necesidad de acceder a los datos. Se autoriza el acceso en función de qué datos resulten necesarios para la finalidad de que se trate; d) Una vez que una administración dispone de la autorización para acceder a unos datos para una finalidad específica, debe autorizar personalmente a los usuarios que realmente efectuarán la consulta; e) Los usuarios autorizados solamente pueden consultar los datos en el contexto de la tramitación de un expediente específico de los que se ajustan a la finalidad autorizada; f) El sistema (la PICA) registra todo lo que ocurre (quién pide, en qué momento, cuándo se obtuvo la respuesta) sin guardar ningún dato concreto de la consulta específica (ni la petición ni la respuesta)".

A partir de este protocolo de actuación, en la consulta se explica que, en la práctica de los últimos años, se han identificado dos situaciones diferentes por parte de un órgano receptor de la información:

En el primer supuesto, el órgano que requiere unos datos o un documento dispone de los datos identificativos del interesado y de la autorización correspondiente, hace la consulta a la PICA y obtiene los datos. En este caso, según el escrito de consulta, es evidente que se produce una comunicación de datos en la que el órgano emisor es el cedente y el receptor es el cesionario (en los términos del artículo 11 de la LOPD).

En el segundo supuesto, en relación con el cual se sitúa la consulta, el órgano que requiere los datos ya dispone de ellos porque se los ha proporcionado la persona interesada y lo que necesita es que el órgano titular de los datos los verifique. En este caso se explica que el órgano requeridor, que ya dispone de los datos, los verifica haciendo una consulta a la PICA, y obtiene una respuesta del tipo *sí/no, consta/no consta*, sin añadir ninguna otra información. Esto, según el escrito de consulta, no implica que el órgano gestor consulte estos datos para incorporarlos al expediente,

porque ya dispone de los datos, simplemente se valida la veracidad de lo declarado por el solicitante.

En este dictamen nos centraremos exclusivamente en el segundo supuesto planteado, que es propiamente el objeto de la consulta presentada.

III

Para analizar la consulta desde la perspectiva de la protección de datos, deberemos tener en cuenta lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), así como, si procede, lo previsto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD (en adelante, RLOPD).

De entrada, es preciso puntualizar el contenido de algunos conceptos de la normativa de protección de datos.

Según la LOPD, suponen un "tratamiento de datos personales" todas las "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias" (artículo 3.c) de la LOPD).

En un sentido amplio, la constatación o verificación de una información personal previamente facilitada por un titular o interesado (en el sentido del artículo 3.e) de la LOPD) afecta a esta información personal, ya que, partiendo de la información que el órgano requeridor ya conocía, la verificación permite confirmar la certeza de esa información.

De hecho, la "verificación" de información personal, en estos términos, es incluso un ejercicio habitual del "tratamiento" de información personal, si consideramos que el principio de calidad (artículo 4 de la LOPD) exige que los datos se traten sólo cuando sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hubieren obtenido. Es más, el artículo 4.3 de la LOPD dispone que los datos de carácter personal deben ser exactos y estar al día, de manera que respondan con veracidad a la situación actual del afectado.

Esta obligación que el artículo 4.3 citado impone al responsable, de oficio, viene a reforzar la consideración de que una verificación de una información personal que ya se posee previamente es una operación que debe considerarse incluida, en un sentido general, en el concepto de "tratamiento de datos personales".

Ahora bien, dicho esto, la consulta se centra en si el ejercicio de verificación en los términos planteados supone una "cesión o comunicación de datos", entendida como cualquier revelación de datos efectuada a una persona distinta del interesado (artículo 3.i) de la LOPD), con las implicaciones que ello tendría desde la perspectiva de la protección de datos.

A efectos explicativos, tomemos el mismo ejemplo que se cita en la consulta: el órgano requeridor ya dispone de los datos del titular (por ejemplo, conoce que forma parte de

una familia numerosa con el número de título correspondiente), y solicita una verificación, simplemente un "sí/no", es decir, contrastar la información. El órgano (Administración Pública) responsable del fichero emite una respuesta "sí/no", o un "consta/no consta", sin añadir nada diferente –otros datos personales complementarios o distintos– de la información personal que ya consta en el expediente del órgano requeridor. Se trata, simplemente, de una validación de la veracidad de la información personal que ya se posee (se trata de una "verificación positiva").

Ciertamente, en este caso, y como se apunta en la propia consulta, podemos entender que no se ha producido una comunicación (o revelación) de datos personales, en la que el órgano requeridor sería el cesionario, sino simplemente una confirmación o validación por parte del órgano que puede contrastar si la información que se posee es veraz.

En el ejemplo citado, de alguna manera se complementa la información que ya se tiene, en el sentido de que se constata la pertenencia de este individuo a una familia numerosa, pero ciertamente no se añade nueva información.

Más allá de este ejemplo, en definitiva, la verificación en estos términos no supone una revelación de "nuevos datos", pues simplemente se informa al órgano que requiere los datos de que la información que ya tenía es correcta o veraz. Se puede interpretar que no se produce una nueva revelación o cesión de datos diferentes a aquellos de los que ya se disponía.

No obstante, convendría puntualizar que, si bien el supuesto planteado puede no ser interpretado como un supuesto de cesión, ello no comporta, como parece derivarse de los términos de la consulta, que "no sería de aplicación la LOPD".

Cada una de las Administraciones u órganos implicados (tanto el órgano requeridor de los datos como el órgano responsable del fichero que contiene los datos) "tratan" información personal, y en este tratamiento se encuentran sometidos a la LOPD.

Por lo tanto, lo que no sería de aplicación, ciertamente, en el supuesto concreto planteado ("verificación positiva") sería el régimen aplicable a las cesiones de datos, previsto en los artículos 11 y 21 de la LOPD, los cuales mencionamos a continuación.

El artículo 11 de la LOPD dispone que los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado (apartado 1). En el apartado 2 del mismo artículo se regulan diversos supuestos en los que el consentimiento que exige el apartado anterior no es necesario, entre otras circunstancias, cuando la cesión está autorizada en una ley.

El artículo 21 de la LOPD regula las particularidades del régimen de comunicación de datos cuando ésta se produce entre Administraciones Públicas, y por tanto resulta de aplicación en el caso que nos ocupa, puesto que las consultas a la PICA tienen, en todo caso, como intervinientes (cedente y cesionario) a Administraciones Públicas. En el artículo 21.1 se prevé que los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el ejercicio de sus atribuciones no deben ser

comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, excepto cuando la comunicación tenga por objeto el tratamiento posterior de los datos con finalidades históricas, estadísticas o científicas. En este caso tampoco es necesario disponer del consentimiento del titular de los datos. El artículo 21.2 de la LOPD establece que, en todo caso, podrán ser objeto de comunicación los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.

Ahora bien, la no aplicación del régimen citado de comunicación de datos personales no se puede extender al resto de principios y obligaciones de la normativa de protección de datos, que deben regir las diferentes fases del tratamiento de datos de carácter personal que realizan los distintos intervinientes.

IV

Ciertamente, puede entenderse que el supuesto concreto que acabamos de comentar no estaría sometido al régimen de las comunicaciones de datos personales (artículos 11 y 21 de la LOPD) si se produce en los términos mencionados. Por tanto, no sería necesario recoger el consentimiento (necesario a menos que se disponga de cobertura en norma con rango de ley) en los términos previstos en los artículos 11 y 21 citados.

Ahora bien, esto es así siempre y cuando realmente se trate de una confirmación de lo que ya se conocía y no se aporte ninguna información nueva ni información distinta de aquella que el órgano requeridor ya poseía.

Este matiz es importante, puesto que hay que distinguir entre este primer supuesto comentado y otros supuestos.

El segundo supuesto sería aquel en el cual se produce una verificación en el sentido contrario al apuntado, en el que se confirmaba la información de la que ya se disponía. En este caso la respuesta tipo “sí/no”, “consta/no consta”, es negativa (podríamos denominarlo “verificación negativa”). La verificación negativa implica, de alguna manera, “modificar la información”, en el sentido de pasar a considerar como incierta, o falsa, o no suficientemente contrastada, aquella información que el interesado habría facilitado inicialmente. Como ejemplo, el hecho de negar o no tener constancia de que esta persona pertenezca a una familia numerosa podría suponer una verificación negativa.

El tercer supuesto sería aquel en el cual el órgano responsable del fichero no sólo no confirma la información inicial (verificación negativa), sino que además “complementa” la información, por ejemplo con otros datos relativos a la verdadera situación del afectado. Se facilita, por ejemplo, información complementaria sobre la situación de la persona que ha solicitado una ayuda acreditando pertenecer a una familia numerosa, por seguir el ejemplo anterior (simplemente a efectos explicativos, podría darse el caso de que el órgano titular de la información informe al órgano que solicita la información sobre el número real de hijos de la persona afectada o sobre anteriores solicitudes de ayuda que hubiera cursado el interesado).

Dejemos a un lado este tercer supuesto, ya que no plantea dudas respecto al hecho de que, al añadirse nueva información de la cual no se disponía inicialmente, se ha

producido claramente una cesión o comunicación de esa información, y por tanto habrá que remitirse al régimen de comunicación de datos de la LOPD.

En cuanto al segundo supuesto, que hemos denominado "verificación negativa", esta Agencia considera que también se trata de una revelación de información o comunicación de datos, a los efectos de la normativa de protección de datos personales. El hecho de que no se confirme positivamente lo que ya conocíamos condiciona y modifica en cierto modo la información de la que ya se disponía. En consecuencia, en este caso también habría que remitirse al régimen citado de comunicación de datos (artículos 11 y 21 de la LOPD).

Ahora bien, incluso en este segundo supuesto (verificación negativa) veremos que el marco normativo aplicable puede dar cobertura suficiente a la comunicación de información personal, como se detallará a continuación.

V

Antes de entrar en las posibles habilitaciones legales de la comunicación de datos en el contexto de las verificaciones negativas, hay que partir de la base de que las consultas a la PICA siempre implican a órganos de Administraciones Públicas (nos referimos al órgano solicitante de información y al responsable del fichero donde se trata la información), sean de la misma Administración o de dos diferentes.

En cada caso es necesario tener en cuenta la naturaleza jurídica del órgano que realiza la petición de verificación a través de la PICA y la del órgano titular del fichero origen de los datos, para ver si pertenecen a la misma Administración Pública o, en su caso, si se puede aplicar alguna de las habilitaciones previstas para la comunicación de datos entre Administraciones Públicas.

A este respecto, el artículo 2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en relación con el ámbito de aplicación de esta ley, dispone que se entiende por Administraciones Públicas, entre otras, las Administraciones de las comunidades autónomas (apartado 1), y añade que las entidades de derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las Administraciones Públicas tendrán asimismo la consideración de Administración Pública (apartado 2).

Esto es relevante en el sentido de que, por ejemplo, la comunicación de datos dentro de la Administración de la Generalitat que implique a un interviniente (cedente o cesionario) que tenga personalidad jurídica propia debe considerarse sometida al artículo 21 de la LOPD, como ha puesto de manifiesto esta Agencia en diversos Dictámenes, entre otros, y a modo de ejemplo, el Dictamen 39/2009 (disponible en la página web: www.apd.cat).

En el caso que nos ocupa, partimos de la base de que muchas peticiones de verificación se producirán entre dos órganos de la Administración de la Generalitat –sin que ninguno de ellos tenga personalidad jurídica propia–, caso que tampoco es propiamente un supuesto de cesión o comunicación de datos en los términos del artículo 3.i) de la LOPD.

En estos casos, lógicamente, si bien no hace falta aplicar el requisito de la recogida del consentimiento, sí es necesario que el tratamiento que pueda realizar el órgano que verifica la información se ajuste al principio de finalidad en los términos del artículo 4.2 de la LOPD, según el cual los datos de carácter personal objeto de tratamiento no se pueden utilizar para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

Respecto al principio de finalidad, en el caso que nos ocupa, podemos considerar que la verificación de una información facilitada por la misma persona interesada (y la obtención de una verificación negativa, en este caso) por parte de un órgano de la Administración puede resultar ajustada a este principio, si la verificación se justifica, con la suficiente concreción, en las competencias o materias que trata este órgano y además la información que se pretende contrastar no se ha recogido con una finalidad que pueda resultar incompatible. Más aún, si tenemos en cuenta la referencia ya hecha al principio de calidad y a la exigencia para el responsable de un tratamiento de datos de mantener actualizada y correcta la información (artículo 4.3 de la LOPD) y vinculamos esta exigencia con el ejercicio de las competencias que pueden hacer necesaria una consulta a la PICA, podemos entender que el órgano que formula la consulta tiene que poder contrastar la información que le ha dado el interesado, y que esta consulta y verificación queda habilitada por los principios mencionados.

Finalmente, en aquellos casos en que la verificación implique dos entes públicos con personalidades jurídicas diferenciadas (caso también probable en el contexto de las consultas a la PICA), habrá que aplicar el régimen general de la LOPD (artículos 11 y 21), tal como veremos a continuación.

VI

Hecha esta consideración respecto a la naturaleza de los intervinientes en las consultas a la PICA, pasamos ya a comentar los supuestos que pueden habilitar la comunicación, en el contexto que analizamos.

Visto el régimen previsto en la LOPD para la comunicación de datos, hay que tener en cuenta diversas previsiones del marco normativo aplicable al supuesto que nos ocupa, en el que la petición de información por parte del órgano solicitante comporta una comunicación o cesión de datos personales. Como ya se ha dicho, el consentimiento del titular no es necesario si se da la suficiente cobertura en una norma con rango de ley, entre otros supuestos (artículo 11.2 de la LOPD).

En cualquier caso, insistimos en que las consideraciones con respecto a la normativa que citaremos a continuación resultarían aplicables al supuesto que hemos denominado "verificación negativa".

De entrada debemos tener en cuenta que el artículo 11.2.c) de la LOPD excluye la necesidad de disponer del consentimiento en el siguiente caso:

> *"Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control impliquen necesariamente la conexión del tratamiento mencionado con ficheros de*

terceros. En este caso, la comunicación sólo será legítima cuando se limite a la finalidad que la justifique".

Este supuesto parte de la existencia de una relación jurídica, entre otras, administrativa (como la que se podría dar entre el ciudadano y la Administración Pública ante la que se realiza un trámite a través del Catálogo). Cuando el desarrollo, cumplimiento y control de la relación jurídica implican necesariamente la conexión (o consulta, en el supuesto que nos planteamos) con ficheros de terceros (en este caso, de la Administración Pública u órgano titular del fichero donde se encuentran los datos), la cesión que se produciría no exigirá el previo consentimiento del titular.

Esto es así no sólo por las consideraciones anteriores sobre los principios de calidad y de finalidad, sino especialmente porque debe tenerse en cuenta que la normativa exige que la Administración realice determinadas comprobaciones de datos. Encontramos una previsión en este sentido en el artículo 78.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, que dispone lo siguiente en relación con la instrucción del procedimiento:

"Los actos de instrucción necesarios para la determinación, conocimiento y ***comprobación de los datos*** *en virtud de los cuales deba pronunciarse la resolución,* ***se realizarán de oficio por el órgano que tramite el procedimiento****, sin perjuicio del derecho de los interesados a proponer aquellas actuaciones que requieran su intervención o constituyan trámites legal o reglamentariamente establecidos".*

Este artículo establece con carácter general la comprobación de información, que debe realizarse de oficio, en relación con los datos necesarios para dictar resoluciones.

La misma Ley 30/1992, citada, contiene previsiones de comprobación o verificación de información en el ámbito más específico de las declaraciones responsables y las comunicaciones previas, en el artículo 71.bis), añadido por el artículo 2.3 de la Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y su ejercicio (denominada "Ley Ómnibus").

En concreto, el artículo 71.bis), en su apartado 3, dispone que:

"Las ***declaraciones responsables y las comunicaciones previas*** *producirán los efectos que se determinen en cada caso por la legislación correspondiente y permitirán, con carácter general, el reconocimiento o ejercicio de un derecho o bien el inicio de una actividad, desde el día de su presentación,* ***sin perjuicio de las facultades de comprobación, control e inspección que tengan atribuidas las Administraciones Públicas. (...)".***

El mismo artículo 71.bis) también dispone, en su apartado 4, que la inexactitud, falsedad u omisión, de carácter esencial, de cualquier dato, manifestación o documento que se acompañe o incorpore a una declaración responsable o comunicación previa determina la imposibilidad de continuar con el ejercicio del derecho o actividad de que se trate, sin perjuicio de las responsabilidades a que hubiera lugar.

El régimen de la declaración responsable y de la comunicación previa debe completarse con la Ley 26/2010, de 3 de agosto, de Régimen Jurídico y de Procedimiento de las Administraciones Públicas de Cataluña. Esta Ley 26/2010, que entra en vigor, con determinadas excepciones, tres meses después de su publicación en el DOGC (5 de agosto de 2010), contiene previsiones sobre la verificación, en relación con la declaración responsable y en relación con la comunicación previa. Los artículos 35 (en relación con la declaración responsable) y 36 (en relación con la comunicación previa), ambos de la Ley 26/2010, citada, disponen lo siguiente:

Artículo 35:

"1. A los efectos de la presente ley, se entiende por ***declaración responsable*** *el documento suscrito por la persona interesada en el que declara, bajo su responsabilidad, que cumple los requisitos establecidos por la normativa vigente para acceder al reconocimiento de un derecho o facultad o para su ejercicio, que dispone de la correspondiente documentación acreditativa y que se compromete a mantener su cumplimiento durante la vigencia de dicho reconocimiento o ejercicio.*

2. La declaración responsable debe incluir los datos relativos a la identificación de quien la suscribe y los requisitos a los que se refiere el apartado 1, que deben hacerse constar, en cada caso, de forma expresa, clara y precisa.

3. Sin perjuicio de los efectos concretos que en cada caso determine la legislación sectorial, ***la presentación de la declaración responsable en el marco de un procedimiento administrativo faculta a la administración pública competente para verificar la conformidad de los datos que en ella se contienen".***

Artículo 36:

"1. A los efectos de la presente ley, se entiende por ***comunicación previa*** *el documento suscrito por la persona interesada con el que pone en conocimiento de la Administración Pública competente hechos o elementos relativos al ejercicio de un derecho o al inicio de una actividad, indicando los aspectos que pueden condicionarlo, y que se acompaña, si procede, de la documentación necesaria para su cumplimiento de conformidad con lo establecido por la normativa sectorial.*

2. Sin perjuicio de los efectos concretos que en cada caso determine la normativa sectorial, la comunicación previa permite el reconocimiento o ejercicio de un derecho o el inicio de una actividad, desde el día de su presentación, y ***faculta a la administración pública correspondiente para verificar la conformidad de los datos que en ella se contienen".***

Por tanto, la normativa citada –si bien en lo que respecta a la Ley 26/2010 hay que esperar a su entrada en vigor— prevé en estos supuestos la facultad de la Administración Pública ("competente" en el artículo 35.3, citado, y "correspondiente" en el artículo 36.2, citado) de verificar la conformidad de los datos aportados por la

persona interesada, y que se contienen en la declaración responsable o en la comunicación previa.

Teniendo en cuenta las previsiones que, en el marco del artículo 71.bis) de la Ley 30/1992, citada, especifica la Ley 26/2010, la normativa prevé determinadas verificaciones de oficio que, al referirse a datos de carácter personal, cuentan con la correspondiente habilitación legal, en el caso de las declaraciones responsables y de las comunicaciones previas, en los términos indicados.

Todas estas previsiones podrían amparar, por lo tanto, y dar la suficiente cobertura a las consultas realizadas a través de la PICA, en el caso de las verificaciones negativas.

Sirvan estos ejemplos, u otros que se puedan contener en otra normativa (por ejemplo, el artículo 24.2 de la Ley 38/2003, de 17 de noviembre, General de Subvenciones, según el cual el órgano competente para la instrucción del procedimiento de concesión de subvenciones realizará de oficio cuantas actuaciones estime necesarias para la determinación, conocimiento y comprobación de los datos en virtud de los cuales debe formularse la propuesta de resolución), para reforzar la consideración hecha respecto de la obligación que se impone a las Administraciones Públicas de comprobar que la información que tratan (a los efectos que nos interesan, la información personal) es veraz, obligación que es coherente con los principios de protección de datos personales previstos en la LOPD.

Con independencia de la previsión del artículo 11.2.c), que hemos comentado, pueden existir también casos en los que para el ejercicio de las mismas competencias, o de competencias que traten las mismas materias (siguiendo la fórmula del artículo 21.1 de la LOPD), la cesión o comunicación de datos, en el contexto de las consultas a la PICA que analizamos, puede encontrar cobertura en el citado artículo 21 de la LOPD, al cual ya nos hemos referido en el presente dictamen.

Esta exposición que hemos hecho debe completarse con lo que se deriva de la Sentencia del Tribunal Supremo, de 15 de julio de 2010 (recurso 23/2008), en concreto, en relación con el artículo 11 del RLOPD. Este artículo se refería a la verificación de datos en solicitudes formuladas a las Administraciones Públicas, en los siguientes términos:

> *"Cuando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias* ***las verificaciones necesarias*** *para comprobar la autenticidad de los datos".*

Este artículo ha sido declarado nulo por la STS citada. En síntesis, la sentencia considera que el artículo 11 del RLOPD no tiene la habilitación legal exigida por los artículos 6 y 11 de la LOPD y que la cobertura necesaria no puede ser genérica, y no puede buscarse, en cualquier caso, en una norma de rango reglamentario.

Los artículos 6.2.b) y 9) de la Ley 11/2007, relativos al derecho de los ciudadanos a no aportar datos y documentos que obren en poder de las Administraciones Públicas, propiamente no se refieren a la posibilidad de "verificación" de datos por parte de la

Administración Pública, y remiten a la LOPD en cuanto a la exigencia de consentimiento o norma con rango de ley para hacer efectivo este derecho de los ciudadanos. En concreto, el artículo 9 de la misma Ley 11/2007 regula expresamente las cesiones de datos entre Administraciones Públicas como sigue:

> *"1. **Para un eficaz ejercicio del derecho reconocido en el apartado 6.2.b)**, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, **de conformidad con lo dispuesto en la Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.*
>
> *2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos. **El acceso a los datos de carácter personal estará, además, condicionado al cumplimiento de las condiciones establecidas en el artículo 6.2.b) de la presente Ley".***

La STS citada analiza expresamente la relación de la previsión del artículo 11 del RLOPD con los artículos 6.2.b) y 9 de la Ley 11/2007, y considera que estos artículos no pueden considerarse la cobertura necesaria para la previsión de verificación del RLOPD, consideración que esta Agencia comparte. Asimismo, se deriva de la STS que no se puede presuponer una cobertura legal de forma general y, en todo caso, la cobertura necesaria no se puede encontrar en una norma de rango reglamentario.

Ciertamente, la STS excluye la posibilidad generalizada de que las Administraciones Públicas realicen comprobaciones sin la suficiente cobertura legal.

No obstante, si, teniendo en cuenta las previsiones legales mencionadas, las comprobaciones o verificaciones que deban realizar las Administraciones Públicas encuentran la suficiente cobertura, estas comprobaciones se ajustarán a lo que exige la normativa de protección de datos. El parecer explicitado en el presente dictamen coincide así con lo que se desprende del marco normativo examinado y de la STS citada, en el sentido de exigir la suficiente cobertura legal para poder proceder a realizar las comprobaciones o verificaciones de información personal que resulten necesarias, y siempre que se cumplan una serie de requisitos, que se comentan a continuación.

VII

Aparte de que, como hemos indicado, y para el supuesto de las verificaciones negativas (y, obviamente, para aquellas verificaciones en las que se complementa la información), el marco normativo aplicable pueda dar cobertura suficiente a la comunicación de información personal, es importante que, con carácter general, y a fin de dar correcto cumplimiento a los principios y garantías de la normativa de protección de datos, las

Administraciones Públicas implicadas en el ejercicio de verificación o comprobación de dato analicen cómo debe realizarse este ejercicio.

Como ya se ha apuntado al referirnos en este dictamen a los principios de calidad y de finalidad, cualquier flujo informativo de datos personales debe limitarse a los datos adecuados, pertinentes y necesarios para la finalidad legítima que resulte pertinente en cada caso.

Esto comporta que, en el contexto que nos ocupa de las verificaciones de información a través de la PICA entre órganos de las Administraciones Públicas, sea aconsejable que, antes de realizar la consulta, se analicen, entre otras, las siguientes cuestiones:

- Cómo y cuándo se formula la consulta: si la consulta (por ejemplo para constatar la información que ha aportado un interesado alegando que forma parte de una familia numerosa) se realiza en relación con cualquier solicitud o bien sólo en determinados casos en los que se considera necesario hacer la verificación; qué elementos hay que tener en cuenta para que se considere necesario hacer la verificación.

Aunque, al describir el procedimiento de acceso a los datos, en la consulta se explica que no se puede acceder a datos de forma genérica, y que siempre se necesita la autorización previa para cada finalidad que justifique la necesidad de acceder a los datos –consideraciones que, sin duda, se ajustan a los principios de protección de datos mencionados–, debemos considerar que existen finalidades que pueden ser más o menos genéricas (por ejemplo, finalidades relacionadas con competencias en materia de servicios sociales). Esto lleva a considerar que lo que se alega en cada caso como motivo de acceso no debería ser una finalidad genérica o formulada en términos amplios. sino concretada en relación con el procedimiento concreto en el que se requiere hacer una verificación.

- Qué información se requiere: en conexión con lo que se acaba de apuntar, a pesar de encontrarnos con diferentes verificaciones que se justifican por el ejercicio de la misma competencia (por parte del órgano requeridor), en cada caso puede ocurrir que los datos concretos que resultan necesarios sean diferentes. Esto puede deberse a que en un caso se haya podido contrastar por otras vías la información que se va a verificar, y en otro caso no.

- A quién se solicita la información: también se debería valorar que, en un supuesto de verificación, las fuentes de información que están en disposición de contrastar los datos pueden ser diversas. Salvo los casos en que hay una única fuente para verificar la información, habrá que analizar previamente qué fuente resulta más adecuada, desde la perspectiva del principio de calidad de los datos. Es decir, habrá que valorar qué fuente puede resultar más fiable para dar una información personal veraz, actualizada y sin errores.

En definitiva, recomendamos que se protocolicen estos y otros aspectos de la verificación, si procede, en la medida de lo posible, y también, teniendo en cuenta la perspectiva de la protección de datos, el procedimiento de acceso a la información que se resume en el escrito de consulta.

Aparte de esto, también se recomienda que el titular de los datos personales objeto de verificación sea, en todo caso, y de forma previa al tratamiento de los datos, consciente de que se puede realizar dicha verificación. Es decir, en términos de la normativa de protección de datos, el titular de los datos debe estar informado previamente de la posibilidad de que se verifique la información que él mismo ha aportado.

Esta recomendación se enmarca, lógicamente, en lo que dispone el artículo 5 de la LOPD, que se refiere en los siguientes términos al deber de información que deben cumplir los responsables de tratar datos personales de los ciudadanos:

> *"1. "Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*
> *a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
> *b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
> *c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
> *d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
> *e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.*
> *Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.*
> *2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en éstos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.*
> *(...)".*

Esto conduciría, concretamente, a que en el momento de recoger los datos de una persona que solicita una ayuda como miembro de una familia numerosa (para seguir el ejemplo que hemos estado utilizando en el presente dictamen), ya sea a través de formularios, impresos, presencialmente o por vía telemática, etc., se le informe, entre otras cosas, de la posibilidad de que la Administración que recoge sus datos (aparte de informar de que estos pasarán a formar parte de un determinado fichero, o de informar de la unidad a la que debe dirigirse para ejercer sus derechos, etc.), se dirija al órgano correspondiente, en el ejemplo puesto el Departamento de Acción Social y Ciudadanía de la Generalitat, para verificar la información. Esta previsión de ulteriores comprobaciones o verificaciones de los datos aportados por el interesado debería incluirse en la correspondiente cláusula informativa que es necesario prever en aplicación del artículo 5 de la LOPD, citado.

Debe tenerse en cuenta que el artículo 5.1.c) de la LOPD dispone que es necesario informar "de las consecuencias de la obtención de los datos...", y podemos considerar que informar sobre el hecho de que la obtención de los datos puede comportar una

verificación posterior es informar sobre una consecuencia posible de la obtención de los datos que facilita el propio interesado.

Aunque es cierto que el propio artículo 5.3 de la LOPD prevé que no es necesario informar, entre otras cosas, de estas consecuencias, si se deduce claramente de la naturaleza de los datos o de las circunstancias en las que se recogen, se puede considerar que puede no ser de general conocimiento por parte de los ciudadanos la posibilidad que tienen las Administraciones Públicas de hacer estas comprobaciones, especialmente a la hora de conocer cuál será la información de contraste. Por eso habría que incluir dicha información en la cláusula informativa correspondiente.

Por todo ello se emiten las siguientes

Conclusiones

La LOPD, y, por tanto, sus principios y garantías, son aplicables a las diferentes fases del tratamiento de datos de carácter personal (según el artículo 3.c) de la LOPD) que realizan las Administraciones Públicas.

El supuesto en que el órgano que requiere los datos ya dispone de ellos porque se los ha proporcionado la persona interesada, y obtiene una "verificación positiva" de la información, sin que se añada ninguna otra información, no supone una revelación de nuevos datos personales, y no se produce una comunicación de datos en los términos del artículo 3.i) de la LOPD.Por lo tanto, no resulta necesario requerir el consentimiento del afectado, que es un requisito previsto en el régimen aplicable a las comunicaciones de datos (artículos 11 y 21 de la LOPD).

El supuesto en que el órgano que requiere los datos obtiene una "verificación negativa", en el sentido de pasar a considerar como incierta, o falsa, o no suficientemente contrastada la información facilitada por el interesado, implica una revelación de datos.

Por lo tanto, en este caso, o bien, obviamente, si se modifica la información inicial o se añade cualquier dato personal complementario, se puede considerar que se ha producido una cesión o comunicación de datos, sometida al régimen general previsto en los artículos 11 y 21 de la LOPD.

En el caso de las verificaciones negativas, las previsiones de la propia normativa de protección de datos (artículos 11.2.c) y 21) de la LOPD) pueden dar suficiente cobertura a las cesiones de datos, sin que sea necesario recoger el consentimiento previo de los interesados. En conexión con el artículo 11.2.c) citado, debe tenerse en cuenta lo previsto en la Ley 30/1992 (artículo 78.1 y artículo 71.bis) y las habilitaciones que se desprenden de la Ley 26/2010 (artículos 35 y 36) o de otra normativa sectorial.

Se recomienda analizar y protocolizar, desde la perspectiva de la protección de datos personales, diversas cuestiones relativas a los términos en los que se realizan las verificaciones a través de la PICA y a los flujos informativos que estas verificaciones pueden producir.
Asimismo, se recomienda informar convenientemente al interesado, en el contexto del deber de información (artículo 5 de la LOPD), sobre la posibilidad de realizar ulteriores comprobaciones o verificaciones de la información personal aportada.