Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

Javier Bikandi Irazabal
Director de Atención a la Ciudadanía e Innovación
y Mejora de la Administración
DEPARTAMENTO DE ADMINISTRACIÓN PÚBLICA Y JUSTICIA
GOBIERNO VASCO
Donostia-San Sebastian, 1
01010 Vitoria-Gasteiz

Erref.
Ref. **IL15-009**

GAIA
ASUNTO

"Euskal Sektore Publikoko Antolamendu eta Funtzionamenduari buruzko Lege-Proiektuari" buruzko txosten juridikoa

Informe jurídico sobre *"el Proyecto de Ley de Organización y Funcionamiento en el Sector Pública Vasco"*

Jaun hori:

Honekin batera bidaltzen dizut Bulegoak egin duen txosten juridikoa zuren kontsultaren gainean.

Adeitasunez.

Vitoria-Gasteiz, 2015eko uztailak 24

Estimado Sr.:

Adjunto le remito informe jurídico elaborado por esta Agencia en relación a la consulta realizada por usted.

Atentamente.

Vitoria-Gasteiz, 24 de julio de 2015

P. D.

DATUAK BABESTEKO EUSKAL BULEGOA
AGENCIA VASCA DE PROTECCIÓN DE DATOS

Joseba Etxebarria Goikoetxea
Idazkari Nagusia / El Secretario General

Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

IL15-009

INFORME QUE FORMULA LA AGENCIA VASCA DE PROTECCION DE DATOS EN RELACION CON EL ANTEPROYECTO DE LEY DE ORGANIZACIÓN Y FUNCIONAMIENTO EN EL SECTOR PUBLICO VASCO

I

ANTECEDENTES

El Director de Atención a la Ciudadanía e Innovación y mejora de la Administración remite el texto del Anteproyecto de ley arriba referenciado para que esta Institución realice las aportaciones que estime oportunas en aras a contribuir a mejorar su calidad.

II

INTERVENCIÓN DE LA AGENCIA VASCA DE PROTECCIÓN DE DATOS

El presente informe se emite en respuesta al trámite de audiencia concedido a esta Agencia Vasca de Protección de Datos

III

CONFIGURACIÓN CONSTITUCIONAL DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

Antes de adentrarnos en el análisis del texto remitido, realizaremos una consideración general sobre la configuración constitucional del derecho fundamental a la protección de datos de carácter personal.

La Constitución de 1978 consagra en su Título I una serie de derechos fundamentales, a los que dota de eficacia jurídica y establece distintos niveles de garantía, a través de instituciones e instrumentos de diferente naturaleza y de diferente alcance. Entre esos derechos, no existe en la CE una referencia expresa al derecho a la protección de datos de carácter personal, pero sí lo contempla en el artículo 18.4 que dispone que *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*.

De ese precepto constitucional deriva el derecho fundamental a la protección de datos de carácter personal o derecho a la autodeterminación informativa, que la jurisprudencia constitucional (por todas, la STC 292/2000, de 30 de noviembre), ha consagrado como derecho fundamental autónomo, cuyo ámbito es más amplio que el derecho a la intimidad.

Así lo ha declarado el Tribunal Constitucional en la Sentencia señalada:

> *"La protección de datos no se reduce sólo a los datos íntimos de la persona, sino cualquier tipo de datos de carácter personal, sean íntimos o no, cuyo conocimiento o*

empleo por terceros puede afectar a sus derechos sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. ...Los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo" (FJ 6º)".

Debe insistirse en que este derecho no se limita a servir de instrumento de garantía de otros derechos frente al uso torticero de la informática, sino que es un derecho fundamental que goza de sustantividad propia y de autonomía con respecto a todos los demás. Confiere a cada persona el pleno dominio sobre el flujo de informaciones que le conciernen, a protegerse frente a potenciales agresiones a la dignidad y a la libertad proveniente de un uso ilegítimo del tratamiento automatizado de datos, y a reaccionar ante ese tipo de actuaciones.

El Tribunal Constitucional viene afirmando *que "se trata, por tanto, de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos"* (SSTC 254/1993, FJ 6º, 11/1998, FJ 4º y 290/2000, FJ 7º).

En consecuencia, este derecho no se confunde con el derecho a la intimidad, ya que el derecho de autodeterminación informativa no queda así limitado como aquél, a la posibilidad legal de rechazar los ataques e injerencias perpetradas por extraños (sentido negativo) en la vida íntima de las personas, sino que adquiere ahora una nueva dimensión (sentido positivo) consistente en el reconocimiento de la libertad de la persona para poder controlar el acceso, tratamiento y circulación de sus datos personales (habeas data), sean estos íntimos o no.

Así lo ha declarado el TC, en el FJ 6ª de la STC 292/2000, al señalar que:

"..., el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. .... El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada,

inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre , F. 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado".

Siguiendo con la configuración que de tal derecho fundamental realiza la misma Sentencia, debe recordarse como declara la existencia de "una segunda peculiaridad" consistente en la atribución a su titular de

"... un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, F. 7)".

El TC, en esta misma STC 292/2000, ha definido el contenido de este derecho fundamental del siguiente modo:

"Consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. (...)" (FJ 7º).

Desde una perspectiva diferente, es necesario también tener en cuenta la doctrina del Tribunal Constitucional respecto a las características que debe reunir la Ley (ordinaria) que incide en un derecho fundamental.

Como expresa el Tribunal Constitucional, la Ley puede vulnerar el derecho fundamental por regular (o afectar) el haz de facultades que componen el contenido del derecho fundamental, prescindiendo de las precisiones y garantías mínimas exigibles a una Ley, sometida al insoslayable respeto al contenido esencial del derecho fundamental, cuyo ejercicio regula.

Así, la STC 292/2000 de 30 de noviembre, ya citada establece que

> *"... Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (* SSTC 57/1994, de 28 de febrero*, F. 6; STC 18/1999 de 27 de febrero, F. 2)... De otro lado, aun teniendo un fundamento constitucional y resultando proporcionadas las limitaciones del derecho fundamental establecidas por una Ley (*STC 178/1985 *), éstas pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación...conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga".*

De la misma manera, el Tribunal Constitucional, en Sentencia 70/2009, se encarga de establecer las características que debe reunir la Ley que proceda a establecer dichos límites, al disponer lo siguiente:

> *"Según jurisprudencia constitucional consolidada, la ley deberá concretar las restricciones, alejándose de criterios de delimitación imprecisos o extensivos, pues vulnera el derecho fundamental a la intimidad personal el establecimiento de límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga (STC 292/2000, de 30 de noviembre, FJ 11). Como señalábamos en la STC 49/1999, en relación justamente con la protección del derecho fundamental a la intimidad, la injerencia en la misma exige de un modo "inexcusable" una previsión legal que "ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención" (FJ 4); ha de poseer lo que en otras ocasiones hemos denominado cierta "calidad de ley" (SSTC 49/1999, de 5 de abril, FJ 5; 169/2001, de 16 de julio, FJ 6; 184/2003, de 23 de octubre, FJ 2)".*

Quiere decirse con lo que antecede, que siendo evidente que el derecho fundamental a la protección de datos no es ilimitado, y que la Constitución ha querido que la Ley "y sólo la Ley", pueda fijar los límites al derecho fundamental, la mera constatación de que la incidencia en el derecho fundamental se produce a través de una Ley no implica, de manera automática, la imposible vulneración del derecho fundamental, sino que deberá comprobarse que dicha Ley cumple los requisitos que la jurisprudencia constitucional exige para hacer válida dicha incidencia.

En definitiva, cualquier límite al derecho fundamental que derive de la ley proyectada, deberá obedecer a una justificación objetiva y razonada, y someterse a la estricta observancia del principio de proporcionalidad en su triple perspectiva de idoneidad, necesidad, y proporcionalidad en sentido estricto.

IV

ANÁLISIS DEL ANTEPROYECTO

A continuación pasaremos a analizar el texto remitido desde la estricta perspectiva que es propia a esta Agencia, esto es, respecto a su adecuación o no al derecho fundamental a la protección de datos personales, y a la normativa que lo regula.

Además, y dada la premura con que se solicita el informe, nos detendremos, exclusivamente, en aquellos aspectos más relevantes que se derivan del anteproyecto remitido.

ESTRUCTURA Y ÁMBITO DE LA LEY

La ley proyectada se estructura en cinco Títulos, ochenta artículos, una Disposición Adicional, una Transitoria, una Disposición Derogatoria y dos Disposiciones Finales.

La primera cuestión que debemos reseñar es la **falta de coincidencia entre el título de la norma legal proyectada, referido al "sector público vasco", y el objeto de la misma,** que según proclama su artículo primero pretende *"regular la organización y funcionamiento de la Administración pública y de todos los entes integrados en* ***el sector público de la Comunidad Autónoma de Euskadi****"*. A tal efecto, este artículo 1.1 del texto entiende por sector público el conjunto formado por la Administración General de la Comunidad Autónoma, la Administración Institucional y los entes instrumentales integrados en la misma.

En segundo lugar, y poniendo en relación el ámbito de la norma proyectada con el ámbito de aplicación de la Ley Vasca 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, debemos destacar que **no todas las entidades que conforman el sector público de la CAE,** y cuyo régimen jurídico regula este anteproyecto de ley, **están sometidas en la actualidad a la Ley Vasca 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.**

Según dispone el artículo 2.1 a) de la Ley del Parlamento Vasco 2/2004, están incluidos en el ámbito de aplicación de esta Ley los ficheros de datos de carácter personal creados o gestionados para el ejercicio de potestades públicas por la Administración General de la Comunidad Autónoma del País Vasco, los órganos forales de los territorios históricos y las administraciones locales del ámbito territorial de la CAPV, así como los entes públicos de cualquier tipo, dependientes o vinculados a las respectivas administraciones públicas, en tanto que los mismos hayan sido creados para el ejercicio de potestades de derecho público.

La redacción de este precepto, resulta ciertamente confusa, permitiendo una lectura restrictiva respecto a la inclusión en su ámbito subjetivo de personificaciones instrumentales jurídico privadas.

Sin embargo, el juego del binomio Ley-Reglamento de desarrollo, en concreto, del artículo 1.1 del Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley Vasca 2/2004, puede permitir entender incluido en su ámbito de aplicación a todos los ficheros creados o gestionados por las entidades incluidas en el artículo 2.1 de la Ley, para el ejercicio de potestades públicas, con independencia de la naturaleza jurídica pública o privada de su titular.

En todo caso, subsiste también otro problema básico, referido al alcance que debe darse al concepto potestades públicas, dado que para entender que los ficheros están sometidos a la norma autonómica y al ámbito de actuación de la AVPD, es necesario demostrar su vinculación con el ejercicio de potestades públicas. Para ello caben dos

opciones, o se retoma la noción material de potestades públicas, entendida como ejercicio de funciones públicas o la prestación de servicios propios de la Administración a la que esas entidades están vinculadas, o habrá de atenderse a su noción formal, entendida como ejercicio de facultades exorbitantes, con fuerza ordenadora y coercitiva.

Lo cierto es que **el ámbito subjetivo de aplicación de la Ley Vasca 2/2004, de 25 de febrero, no está suficientemente resuelto en la norma autonómica vigente**, y sería aconsejable una redacción más clarificadora de su alcance.

Todo indica que esa redacción del artículo 2.1 de la Ley 2/2004, obedeció a que se trasladó a la norma autonómica la interpretación restrictiva del artículo 41 de la LOPD, abonada por la doctrina de la STC 290/2000, y los pronunciamientos de la AEPD. Sin embargo, creemos posible que la ley autonómica lleve a cabo una reinterpretación de este artículo 41 de la LOPD, igualmente respetuosa con el texto constitucional, pero más acorde con los principios que rigen el modelo territorial de Estado.

Con todo lo anterior, lo que se trata de poner de manifiesto es que **con la regulación actualmente vigente, quedarán fuera del ámbito de la Ley 2/2004, y por ende, del control de la Agencia Vasca de Protección de Datos (artículo 17.1 de esa Ley) aquellas entidades que integren el sector público de esta Comunidad Autónoma que no ejerzan potestades públicas.** Nos referimos, en todo caso, a las sociedades de capital (artículo 41 del anteproyecto) y a las fundaciones del sector público de la CAE (artículo 42 del anteproyecto). En consecuencia, los tratamientos de datos de carácter personal que realicen esas entidades estarán sometidos al control de la Agencia Española de Protección de Datos, salvo cuando las mismas actúen en calidad de encargados del tratamiento por cuenta de las Administraciones a las que estén vinculadas.

Por todo ello, a juicio de esta Agencia, sería aconsejable la revisión del artículo 2 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, al objeto de analizar la posible extensión de su ámbito de aplicación a todo el sector público de la Comunidad Autónoma de Euskadi.

REGISTRO DE ENTIDADES DEL SECTOR PÚBLICO DE LA COMUNIDAD AUTÓNOMA DE EUSKADI

En el artículo 58 de la norma se crea el Registro de entidades del sector público de la Comunidad Autónoma de Euskadi, disponiendo el apartado tercero que el registro tendrá carácter público y naturaleza informativa. El contenido de los asientos, las formas de acceso al Registro y la coordinación con el resto de registros administrativos existentes se determinará por un desarrollo reglamentario posterior.

Entre la información que preceptivamente debe inscribirse en este Registro, figura la identificación de las personas físicas que formen parte de los órganos de gobierno y administración de la entidad. Además, de conformidad con el apartado sexto de este artículo, toda persona que en el desempeño de sus funciones en la Administración General de la CAE o en cualquier otra entidad del sector público de la CAE sea convocada para participar en el órgano de gobierno o administración de cualquier otra entidad, deberá hacer constar en el Registro su designación e inscripción en dicho cargo.

Pues bien, en la medida en que este Registro contenga datos de carácter personal, constituirá un fichero, sometido a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD). Por ello, deberán cumplirse los requisitos que para la creación e inscripción de los ficheros públicos, recoge el artículo 20 de la LOPD. Asimismo, todo tratamiento de esos datos personales, deberán cumplir las prescripciones contenidas en esa Ley Orgánica y su normativa de desarrollo (en especial, los principios de información, calidad, consentimiento, seguridad y deber de secreto).**La indeterminación actual del contenido de los asientos, al quedar relegada a un desarrollo reglamentario posterior, impide a esta Agencia valorar la proporcionalidad de los datos personales que se incluirán en el Registro y los que se pondrán a disposición del público**.

FUNCIONAMIENTO DEL SECTOR PÚBLICO DE LA CAE AL SERVICIO DE LA CIUDADANÍA

El capítulo primero del Título V recoge un catálogo de principios de funcionamiento del sector público de la CAE e interacción con la ciudadanía, y los derechos y deberes de la ciudadanía en sus relaciones con ese sector público. Llama la atención que entre esos principios de funcionamiento del sector público de la CAE, recogidos en el artículo 64, no se incluya la confidencialidad y la protección de datos de carácter personal, y por el contrario, el proyecto, en su artículo 65.5 f), lo contemple expresamente como un deber de los ciudadanos.

El respeto a la protección de datos de carácter personal figura como uno de los principios de la Administración Electrónica (art. 69.l); sin embargo, el respeto al derecho fundamental es un principio que debe inspirar el funcionamiento de todo el sector público, con independencia de que los tratamientos de datos se realicen por medios electrónicos o de otro tipo.

ADMINISTRACIÓN ELECTRÓNICA Y ATENCIÓN CIUDADANA

El texto de la ley proyectada dedica el capítulo tercero del Título V a la Administración electrónica y atención ciudadana.

La Ley 11/2007, de acceso electrónico de los ciudadanos, recoge el respeto al derecho a la protección de datos personales, como el primero de los principios a los que debe ajustarse la utilización de las tecnologías de la información (artículo 4 a).

La intensa vinculación entre la utilización de la informática y el derecho a la protección de datos tiene incluso reflejo constitucional, al haber sido este derecho una creación jurisprudencial realizada a partir del artículo 18.4 de la Constitución Española.

Debemos ahora detenernos en el artículo 73 del texto remitido, relativo a la simplificación de procedimientos administrativos mediante servicios y canales electrónicos. Los apartados uno y dos de este precepto disponen lo siguiente:

> *"1.- Con el fin de simplificar la tramitación administrativa y de garantizar el derecho de la ciudadanía a no aportar los datos y documentos que obren en poder de las Administraciones Públicas, no se recabará el consentimiento de las personas interesadas cuando, en el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias:*

a) *la información que se solicite figure como requisito en la norma que regula el procedimiento administrativo.*
b) *El procedimiento administrativo se inicie a instancia de parte, conllevando por tanto la solicitud por parte del interesado.*
c) *La información esté disponible en la Administración General de la Comunidad Autónoma de Euskadi o en los servicios de interoperabilidad entre administraciones, y*
d) *no se refiera a datos de carácter personal especialmente protegidos.*

2. En los supuestos en que así lo prevean las normas reguladoras de los procedimientos administrativos, el cumplimiento de los requisitos podrá justificarse a través de la presentación electrónica de una declaración responsable o de las comunicaciones previas, que producirán los efectos que se determinen en cada caso por la legislación correspondiente".

A nuestro juicio, este precepto de la ley incurre en errores que ya han sido puestos de manifiesto por la Agencia en numerosos dictámenes, disponibles en su página web. En ellos recordábamos que el artículo 35 f) de la Ley 30/1992, reconoce el derecho a no presentar documentos que ya se encuentren en poder de la Administración actuante, y que se trata de un derecho y no de una obligación, sin que pueda eliminarse la opción de que sea el propio ciudadano quien acredite el requisito.

Añadíamos también, que la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos, recoge en el artículo 6.2 b) una previsión similar a la incluida en el art. 35 f) de la Ley 30/92 cuando reconoce el derecho de los ciudadanos: *"A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos".*

Sin embargo, como puede observarse, la Ley 11/2007 va más lejos que la Ley 30/1992, puesto que el derecho a no aportar documentos ya no se limita a la Administración actuante, sino que se amplía también a otras Administraciones, cuando esos documentos se encuentren en soporte electrónico. En todo caso, es necesario insistir en que la Ley 11/2007, lo que hace es reconocer un derecho para el ciudadano y no una obligación, de modo que en ningún caso puede eliminarse la opción de que sea el propio ciudadano el que acredite el requisito de que se trate en cada caso.

Este derecho a no aportar datos y documentos, ha sido desarrollado en el ámbito de la Administración Pública de la Comunidad Autónoma de Euskadi mediante el Decreto 21/2012 de 22 de febrero, de Administración Electrónica, que avanza aún más en el respeto a la privacidad en el ejercicio del derecho de los ciudadanos a no aportar documentos o datos obrantes en otras Administraciones Públicas, al exigir que el consentimiento otorgado sea específico e individualizado para cada procedimiento concreto.

En definitiva, **el consentimiento del afectado se constituye como título habilitante para la transmisión de los datos en aquellos supuestos en los que los ciudadanos**

ejerciten su derecho a no aportar datos o documentos que obren en poder de las Administraciones Públicas.

Distinto a este derecho es la facultad de la Administración que tramita un procedimiento administrativo **de comprobar o verificar los datos de los ciudadanos que toman parte en el mismo.**

Esa comprobación, sin consentimiento del interesado, podrá hacerse única y exclusivamente si la misma encuentra amparo suficiente en una norma con rango de ley (sea esta una ley general o especial)

La necesidad de que sea una ley la que legitime ese tratamiento de datos ha sido reconocida por TS en Sentencia de 15 de julio de 2010, cuando anula el artículo 11 del Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el reglamento de desarrollo de la LOPD, que bajo el título *"Verificación de datos en solicitudes formuladas a las Administraciones Públicas"* establecía que *"Cuando se formulen que 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".*

El TS declara nulo ese precepto por considerar que no se ajusta a lo dispuesto en los artículos 6, 11 y 21 de la LOPD y 6.2 b) y 9 de la Ley 11/2007, y lo hace precisamente en atención a que el rango reglamentario de esa norma no es suficiente para legitimar tratamientos no consentidos de datos personales.

Todas estas consideraciones deberán necesariamente ser tenidas en cuenta por el legislador para conciliar el derecho de las personas a no aportar documentos, con su derecho a la privacidad.

Continuando con el artículo 73 del proyecto, debemos ahora detenernos en sus tres últimos apartados, que establecen lo siguiente:

> *"4.- Cuando las personas interesadas en un procedimiento sean desconocidas, se ignore el lugar de la notificación o el medio para hacerlo, o bien, intentada la notificación, no se hubiese podido practicar, la notificación se hará por medio del tablón electrónico de anuncios del sector público de la Comunidad Autónoma de Euskadi, además de por los medios habituales contemplados en la normativa aplicable al procedimiento correspondiente.*
>
> *5.- Cuando se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo, sin perjuicio de la publicación en el perfil del contratista o en los Boletines Oficiales correspondientes, se utilizará el tablón electrónico de anuncios del sector público de la Comunidad Autónoma de Euskadi, lo que se indicará en las correspondientes convocatorias del procedimiento.*
>
> *6.- Las normas reguladoras de las ayudas y subvenciones podrán determinar la publicación de las resoluciones de concesión y sus modificaciones en el tablón electrónico de anuncios del sector público de la Comunidad Autónoma de Euskadi".*

En lo referente al apartado cuatro, resulta obligado mencionar la modificación operada en el artículo 59.5 de la Ley 30/92 de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, por el artículo 25 de la Ley 15/2014, de 16 de septiembre, de racionalización del Sector Público y otras

medidas de reforma administrativa. Fruto de esta modificación, **la notificación**, en los supuestos previstos en el artículo 73.4 de la norma proyectada, **deberá necesariamente realizarse por medio de un anuncio publicado en el Boletín Oficial del Estado, sin perjuicio de que las Administraciones Públicas puedan establecer con carácter facultativo, otras formas de notificación complementarias.**

En cuanto a la previsión del apartado cinco, relativa a **la publicación de los actos integrantes de un procedimiento selectivo o de concurrencia competitiva**, ha de recordarse el criterio expuesto en numerosas ocasiones por la Agencia Vasca de Protección de Datos, consistente en que **los actos de trámite de estos procedimientos debieran ser objeto de una publicidad limitada** a aquellas personas que tomen parte en los mismos, a través de mecanismos tales como la asignación de usuario, contraseña, etc.

Por último, en todo caso, las previsiones de los artículos 73.5 y 6 deberán **cohonestarse con las obligaciones de publicidad activa que,** para las ayudas y subvenciones **impone el borrador de proyecto de ley de transparencia,** participación ciudadana y buen gobierno del sector público vasco.

Debe además tenerse en cuenta que el artículo 8.1.c) de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, establece con carácter básico, la obligación de hacer públicas en las correspondientes sedes electrónicas o páginas web, las subvenciones y ayudas públicas concedidas con indicación de su importe, objetivo o finalidad y beneficiarios.

En este sentido, resulta de interés mencionar la **Sentencia del Tribunal de Justicia de la Unión Europea, de 9 de noviembre de 2010, sobre publicación de beneficiarios de ayudas** agrícolas, donde el Tribunal precisa que la transparencia debe estar siempre ponderada con el derecho fundamental a la protección de datos de carácter personal.

El asunto lo plantearon un agricultor y una empresa agrícola que demandaron al Land Hessen (Estado Federal de Hessen) por la publicación en el sitio web de la Agencia Federal de Agricultura y Alimentación de sus datos personales, en cuanto beneficiarios de fondos procedentes del FEAGA o del Feader.

Si bien esa publicación de datos venía previamente informada y autorizada por un formulario en el que los afectados reconocían haber sido informados de que el Reglamento (CE) 1290/2005, obliga a publicar los datos de los beneficiarios de fondos procedentes del FEAGA y del Feader y los importes recibidos, el sitio web de la Agencia Estatal recogía lo siguientes datos: Los nombres de los beneficiarios de las ayudas, la localidad en la que están establecidos o en la que residen; el código postal de dicha localidad y los importes anuales recibidos. Dicho sitio web dispone de una función de búsqueda.

Este asunto termina en el Tribunal de Justicia de la Unión Europea donde fue remitido por el juzgado alemán como cuestión prejudicial. El Tribunal de Justicia recrimina, en este caso, que no se hayan tomado en consideración otras formas de publicación de la información relativa a los beneficiarios afectados que respetasen el objetivo perseguido por dicha publicación y, al mismo tiempo, fueran menos lesivas para el derecho a la protección de sus datos de carácter personal.

Por ello, el Tribunal de Justicia de la UE sentencia que se han sobrepasado los límites que impone el respeto del principio de proporcionalidad, al obligar a publicar los nombres de todas las personas físicas beneficiarias de ayudas del FEAGA y del Feader y los importes específicos percibidos por ellas, sin establecer distinciones en función de criterios pertinentes, tales como los períodos durante los cuales dichas personas han percibido estas ayudas, su frecuencia o, incluso, el tipo y magnitud de las mismas.

En definitiva, para el Tribunal de Justicia de la UE no cabe atribuir una primacía automática a la transparencia frente al derecho a la protección de datos personales, sino que es necesario establecer criterios de publicación menos lesivos que permitan conjugar el principio de publicidad y transparencia en la actividad administrativa con el derecho de las personas a la protección de sus datos de carácter personal.

Por último, queremos finalizar este informe con una mención a la reutilización de la información, a la que se refiere el artículo 69 i) del proyecto como uno de los principios de la Administración electrónica. Recientemente se ha aprobado **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**. Esta ley, que tiene carácter de legislación básica, traspone al ordenamiento jurídico interno la nueva Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013.

En la aplicación de este principio de reutilización habrán de observarse las previsiones contenidas en esa ley y, entre ellas, destacaremos el artículo 3 en su nueva redacción, que **excluye del concepto de reutilización el intercambio de documentos entre Administraciones y organismos del sector público, en el ejercicio de las funciones públicas que tengan atribuidas.** (Artículo 3.1 in fine).

Este mismo precepto legal, prescribe que **la reutilización no será aplicable**, entre otros, **a *"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"* (Artículo 3 j).

En Vitoria-Gasteiz, 24 de julio de 2015

DATUAK BABESTEKO EUSKAL BULEGOA
AGENCIA VASCA DE PROTECCIÓN DE DATOS

Iñaki Pariente de Prada
Director de la Agencia Vasca de Protección de Datos