Datuak Babesteko
Euskal Bulegoa

Agencia Vasca de
Protección de Datos

IL15-001

INFORME QUE FORMULA LA AGENCIA VASCA DE PROTECCION DE DATOS EN RELACION CON EL BORRADOR DE ANTEPROYECTO DE LEY SOBRE ADECUACIÓN DE LA LEGISLACIÓN ANTIDOPAJE AL CÓDIGO MUNDIAL ANTIDOPAJE.

ANTECEDENTES

Se somete a informe de la Agencia Vasca de Protección de Datos el Anteproyecto de Ley citado en el encabezamiento.

El presente dictamen se formula en virtud de lo previsto en el artículo quinto 3 b) de la Resolución de 28 de noviembre de 2005, del Director de la Agencia Vasca de Protección de Datos por la que se desarrolla la estructura orgánica de la Agencia Vasca de Protección de Datos, en cuya virtud corresponde a la Unidad de Asesoría Jurídica e Inspección de la misma:

> *"Informar todos aquellos proyectos de disposiciones sobre los que, en relación con la protección de datos personales, le sea solicitado informe".*

CONSIDERACIONES

I

Constituye el objeto de la norma proyectada la adecuación de la Ley Vasca 12/2012, de 21 de junio, de lucha contra el dopaje en el Deporte, al nuevo Código Mundial Antidopaje.

La exposición de motivos de la disposición legal proyectada, señala también como objeto de esta Ley reconocer a la Agencia Vasca Antidopaje como el órgano especializado encargado de desarrollar las funciones atribuidas en el artículo 10 de la Ley a la Administración Pública Vasca, actuando como la organización antidopaje del País Vasco. Además, esta norma legal persigue incorporar a la Ley Vasca 12/2012, el contenido del acuerdo de la Comisión Bilateral de Cooperación Administración del Estado-Administración de la Comunidad Autónoma del País Vasco en relación con esa Ley.

La Ley proyectada cuenta con un artículo único, de modificación de la Ley 12/2012, de 21 de junio, una disposición transitoria y una final.

II

Este informe realizará el análisis del borrador de anteproyecto de ley desde la estricta perspectiva que es propia a esta Agencia, esto es, su ajuste o no a la normativa de protección de datos de carácter personal, sin incidir en cuestiones de legalidad ordinaria ajenas a esta materia.

La regulación de derecho fundamental a la protección de datos de carácter personal se contiene, básicamente, en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal (LOPD, en adelante) y en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba su reglamento de desarrollo. Esta regulación se completa en el ámbito de la CAPV con 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, y su normativa de desarrollo.

Procederemos, en consecuencia, a analizar la adecuación del anteproyecto a los principios y garantías del derecho fundamental a la autodeterminación informativa, si bien, con carácter previo, realizaremos unas consideraciones generales sobre la configuración constitucional de este derecho y hablaremos por su relevancia en esta ley, de los datos de salud y del régimen jurídico aplicable al tratamiento de estos datos.

III

Configuración constitucional del derecho fundamental a la autodeterminación informativa

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 si contempla 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 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 y autónomo y que alguna doctrina ha denominado nuevo derecho fundamental del siglo XXI.

Este derecho fundamental a la protección de los datos personales es un concepto cuyo ámbito es más amplio que el derecho a la intimidad. Así lo ha declarado el Tribunal Constitucional en su STC 292/2000:

> *"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 6ª)".*

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. Así, 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 6° y 11/1998, FJ 4° y la más reciente STC 290/2000, FJ 7°).

En consecuencia, este derecho no se confunde con el derecho a la intimidad ya que el nuevo 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 FD 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 la misma 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 290/2000, 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, porque como expresa el Tribunal Constitucional la Ley puede vulnerar el derecho fundamental por haber regulado (o afectado) 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 se encarga de establecer las características que debe reunir la Ley que proceda a establecer dichos límites.

Así, la Sentencia 70/2009, de acuerdo con la cual

> *"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 el consentimiento es el principio general de protección de datos, que puede ser excepcionado cuando así lo prevea una norma con rango formal de ley que cumpla los requisitos que la jurisprudencia constitucional exige para hacer válida la excepción al consentimiento del interesado. Por ello, siendo evidente que, por una parte, el derecho fundamental a la protección de datos no es ilimitado, y, por otra, que la Constitución ha querido que la Ley "y sólo la Ley", pueda fijar los límites al derecho fundamental, no lo es menos que no resulta suficiente con que los límites se contengan en una norma con rango de Ley, sino que es necesario el cumplimiento de otras exigencias respecto al contenido de la Ley que establezca dichos límites porque también conculcará el derecho fundamental la Ley que limita el derecho fundamental de tal forma que lo haga impracticable, o ineficaz la garantía que la Constitución le otorga.

IV
Datos de Salud

Datos de salud y protección de datos de carácter personal

El concepto *"datos de salud"*, *"datos relativos a la salud"* o, últimamente, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD *"datos de carácter personal relacionados con la salud"* viene definido (artículo 5.1 g) del Real Decreto 1720/2007) como *"las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo"*.

Se establece así un concepto amplio de los mencionados datos siguiendo lo señalado en la Memoria Explicativa del Convenio 108 del Consejo de Europa de 28 de enero de 1981 y las recomendaciones adoptadas por el Comité de Ministros de la citada institución así como la propia jurisprudencia del Tribunal de Justicia de las Comunidades.

En este sentido, el Considerando 45 del Convenio define los datos de salud como *"las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo"*.

De la misma manera, la Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de noviembre de 2003, establece que:

> *"Es preciso dar una interpretación amplia de la expresión datos de salud, empleada por el artículo 8 apartado 1 de la Directiva 95/46/CE de modo que comprende la*

información relativa a todos los aspectos tanto físicos como psíquicos de la salud de una persona".

Dicha interpretación amplia del concepto es ofrecida también por la Recomendación R (97) 5 de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre protección de datos médicos, a cuyo tenor se entiende por tales no solo *"todos los datos personales relativos a la salud de un individuo"*, sino también *"a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos".*

Resulta muy clarificador al respecto el Documento de Trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (Documento EP131) elaborado por el Grupo del artículo 29, de acuerdo con el cual

> *"Esta definición (*la de dato relativo a la salud) *también se aplica a los datos personales cuando tienen una relación clara y estrecha con la descripción del estado de salud de una persona... especialmente si están incluidos en un expediente médico. También habrá que considerarse sensibles otros datos, por ejemplo los datos administrativos (número de seguridad social, fecha de ingreso en un hospital, etc....) contenidos en la documentación médica relativa al tratamiento de un paciente; si no fueran pertinentes en el contexto del tratamiento del paciente, no se habrían incluido, ni deberían haberse incluido en un expediente médico".*

De la misma manera se establece en tal documento que

> *"Las disposiciones jurídicas que introducen un sistema de HME debe establecer por norma general el consentimiento previo del paciente para la introducción de datos en un HME o el acceso a tales datos (especialmente por lo que respecta al tratamiento de datos susceptibles de utilizarse de forma perjudicial, como por ejemplo datos psiquiátricos, datos sobre abortos, etc.), y prever la posibilidad de denegación por lo que respecta a datos menos íntimos".*

Para concluir que

> *"Todos los datos contenidos en documentos médicos, en historiales médicos electrónicos y en sistemas de HME son datos personales sensibles. Por tanto no sólo están sujetos a todas las normas generales sobre protección de datos personales de la Directiva, sino también a las normas sobre protección de datos especiales que rigen el tratamiento de la información sensible, contenidas en el artículo 8 de la Directiva".*

Que los datos de salud se encuentran dentro del ámbito protegido por la intimidad personal es doctrina reiterada del Tribunal Constitucional (últimamente las Sentencias 70/2009 de 23 de marzo y 159/2009 de 26 de junio.)

Dichos datos son también objeto de protección desde la perspectiva del derecho fundamental a la protección de datos de carácter personal.

Así la Sentencia del Tribunal Constitucional 202/1999, de 8 de noviembre, de acuerdo con la cual

> *"Dicho esto, y teniendo en todo momento presente que la concreta cuestión suscitada en el presente recurso de amparo se refiere a la conformidad con el art. 18 CE del tratamiento y conservación en el preciso soporte informático de los datos atinentes a la salud del trabajador, a que se acaba de hacer referencia, debemos señalar que la realización de dichas actividades prescindiendo del consentimiento expreso del afectado ha de calificarse como una medida inadecuada y*

desproporcionada que conculca por ello el derecho a la intimidad y a la libertad informática del titular de la información.

..., lo verdaderamente relevante es que la medida adoptada por la empresa, sometida a los cánones establecidos para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, no reviste la consideración de solución idónea, necesaria y proporcionada para la consecución del fin , en este caso, el control del absentismo laboral [SSTC 66/1995), fundamento jurídico 5°; 207/1996, fundamento jurídico 4° E) y 69/1999), fundamento jurídico 4°], pues no se trata de medida de suyo ponderada y equilibrada, ya que de ella no se derivan más beneficios o ventajas para el interés general o para el interés empresarial que perjuicios sobre el invocado derecho a la intimidad.

Al respecto, interesa recordar que, en desarrollo de lo previsto en el art. 18.4 CE, en la LORTAD se enuncian, entre otros principios generales de la protección de datos, la congruencia y racionalidad de su utilización, «en cuya virtud ha de mediar una nítida conexión entre la información personal que se recaba y trata informáticamente y el legítimo objetivo para el que se solicita y, en consecuencia, prohíbe tajantemente el uso de los datos para finalidades distintas de las que motivaron su recogida (aps. 1 y 2 del art. 4)» (STC 94/1998, fundamento jurídico 4°), así como su exactitud y puesta al día (art. 4.3). Esta regulación es sustancialmente coincidente con lo dispuesto en los arts. 5 y 7 del Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado por España mediante Instrumento de 27 de enero de 1984, y en los arts. 6 y ss. de la Directiva 95/46/CE, de 24 de octubre de 1995), sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Pues bien, en este caso debemos afirmar que el expresado tratamiento informático -con vistas a su conservación- de los datos referidos a la salud de los trabajadores de que tenga conocimiento la empresa quiebra la aludida exigencia de nítida conexión entre la información personal que se recaba y el legítimo objetivo para el que fue solicitada.

Consiguientemente, debemos concluir que el tratamiento y conservación del diagnóstico médico en la mencionada base de datos sin mediar consentimiento expreso del afectado incumple la garantía que para la protección de los derechos fundamentales se contiene en el art. 53 CE".

En el mismo sentido, la Sentencia del Tribunal Europeo de Derechos Humanos de 17 de julio de 2008 establece al respecto que

"La protección de datos personales, en concreto de los datos médicos, es de esencial importancia en el disfrute de un individuo del derecho al respeto de su vida privada y familiar, tal y como garantiza el artículo 8 del Convenio. Respetar la confidencialidad de los datos médicos es un principio vital en los sistemas legales de los Estados Contratantes del Convenio. Es crucial, no solo respetar el sentido de la privacidad de un paciente, sino también, preservar su confidencialidad en la profesión médica y en los servicios de salud en general... La legislación interna debe proporcionar las garantías adecuadas para prevenir cualquier tipo de comunicación o revelación sobre los datos personales de salud, ya que se incumplirían las garantías del artículo 8 del Convenio".

También el Tribunal Constitucional ha señalado que tal derecho fundamental no es ilimitado

> *"... y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7;, F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que* ***la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental.*** *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" STC 292/200".*

Y ha señalado también la manera en que se puede llevar a cabo dichas limitación

> *"De igual modo, respecto al derecho a la protección de datos personales cabe estimar que* ***la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública.*** *Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido.* ***Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias.*** *Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación.".*

Régimen jurídico de la protección de los datos de salud

El Convenio nº 108 del Consejo de Europa de 28 de enero de 1981 establece en su artículo 6 que

> *"Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas".*

Debe ser igualmente objeto de cita el Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la biología y la

medicina, hecho en Oviedo el 4 de abril de 1997 y ratificado mediante Instrumento de 23 de julio de 1999 (BOE nº 251 de 20 de octubre de 1999) que constituye el primer instrumento internacional que trata el derecho a la información, el consentimiento informado y la intimidad de la información relativa a la salud de las personas estableciéndose un marco común para la protección de los derechos humanos y la dignidad en el campo de la biología y la medicina, configurándose en su artículo 5 como regla general para una intervención en el ámbito de la sanidad el consentimiento informado de la persona afectada.

El artículo 8.1 de la Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo referente al tratamiento de los datos personales y a la libre circulación de estos datos, y en cuanto su considerando 33 reconoce que tal tipo de datos relativos a la salud constituyen *"datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad"* establece que

> *"Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad".*

La especial protección conferida a los datos de salud por las normas internacionales y comunitarias tienen reflejo en la LOPD que establece un régimen jurídico específico contenido básicamente en el apartado 3 del artículo 7, artículo dedicado a los *"datos especialmente protegidos"* merecedores del más alto nivel de protección por afectar a los aspectos más íntimos de la personalidad, situándose en un plano en el que confluyen dos derechos fundamentales: el de intimidad y de protección de datos de carácter personal.

De acuerdo con tal apartado.

> *"Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".*

Dada la incidencia especial de los datos de salud, como datos sensibles, en la esfera íntima del afectado, la LOPD ha establecido una regulación específica y más rigurosa que la establecida con carácter general tanto en lo referente a los supuestos en que será posible el tratamiento de los datos como en lo que atañe a las medidas que habrán de adoptarse para garantizar la seguridad en el tratamiento de los datos, así como el cumplimiento de deberes de confidencialidad y sigilo que deben regir en el mencionado tratamiento, de tal manera que la necesidad de obtener el consentimiento expreso de los titulares de tales datos constituye la regla general para el tratamiento de los mismos.

No obstante, el mismo artículo 7.3 contempla la posibilidad de que dicho tratamiento pueda llevarse a cabo en los supuestos en los que una ley así lo disponga debiendo quedar dicha habilitación fundada en la existencia de razones de interés general.

Conviene profundizar en el significado de la expresión *"...solo...cuando...así lo disponga una ley".*

En tal sentido debiera comenzarse otra vez por la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas

físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

De acuerdo con el apartado 4 del artículo 8 de la misma,

> *"Siempre que dispongan las garantías adecuadas los Estados miembros podrán por motivos de interés público importantes establecer otras excepciones además de las previstas en el apartado 2 bien mediante su legislación estatal, bien por decisión de la autoridad de control".*

El Considerando 34 de la Exposición de Motivos de la Directiva 95/46/CE contiene la explicación de dicho precepto. De acuerdo con tal considerando *"se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde no obstante prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas".*

Por su parte, el Grupo de Trabajo sobre protección de datos del artículo 29, en el documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos, ha interpretado también el artículo 8.4 de la Directiva y ha entendido que

> *"En cada caso, el conjunto de tratamientos de datos objeto de excepción deberá presentar un interés público importante para el Estado miembro y dicho tratamiento deberá ser necesario a la luz de tal interés público importante. Este tipo de medidas deben ser proporcionadas es decir no deben existir otras medidas que supongan menos excepciones.*
>
> *Además para que una interferencia con el derecho a la vida privada y familiar sea legítima, deberá ser conforme con el artículo 8 del Convenio Europeo sobre Derechos Humanos y deberá entenderse a la luz de la jurisprudencia de Estrasburgo: debe hacerse de conformidad con la ley y ser necesaria en una sociedad democrática a efectos de un interés público. La jurisprudencia de Estrasburgo ha afirmado en varias ocasiones que la ley que establezca la excepción debe indicar el alcance del poder discrecional conferido a las autoridades competentes y la forma de su ejercicio con la suficiente claridad teniendo en cuenta el objetivo legítimo de la medida en cuestión, a fin de proporcionar al individuo una protección adecuada contra la arbitrariedad".*

El apartado 3 del artículo 8 de dicha Directiva proyecta la anterior previsión a los datos de salud estableciendo que

> *"El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto".*

El punto 7, apartado primero de la Recomendación R (97) de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados Miembros sobre Protección de Datos Médicos trata precisamente de la comunicación de este tipo de datos, estableciendo como regla general en cuanto a su comunicación que *"Los datos médicos no se comunicarán salvo en las condiciones establecidas en este capítulo y en el Capítulo 12".*

El apartado tercero de dicho punto, en lo que ahora más puede interesar, contempla dos supuestos en los que es posible la comunicación de dichos datos sin el consentimiento de su titular:

> *"a) cuando la comunicación esté prevista por una Ley y constituya una medida necesaria en una sociedad democrática por:*
>
> *i. razones de salud pública; o*
>
> *ii. la prevención de un peligro real o la represión de un delito específico; o*
>
> *iii. otro interés público importante; o*
>
> *iv. la protección de los derechos y libertades de otros*
>
> *b) cuando la comunicación sea permitida por una Ley con fines de:*
>
> *i. protección del sujeto de los datos o de un pariente en línea genética*
>
> *ii. salvaguarda de intereses vitales del afectado o de una tercera persona; o*
>
> *iii. el cumplimiento de obligaciones contractuales específicas; o*
>
> *iv. el establecimiento, ejercicio o defensa de una reclamación legal".*

El documento WP131 al que se ha hecho referencia más arriba, señala igualmente que

> *"Esta excepción cubre solamente el tratamiento de datos personales para el propósito específico de proporcionar servicios relativos a la salud de carácter preventivo, de diagnóstico, terapéutico o de convalecencia y a efectos de la gestión de estos servicios sanitarios como por ejemplo facturación, contabilidad o estadísticas.*
>
> *No se cubre el tratamiento posterior que no sea necesario para la prestación directa de tales servicios, como la investigación médica, el reembolso de gastos por un seguro de enfermedad, o la interposición de demandas pecuniarias. También queda fuera del alcance de la aplicación del apartado 3 del artículo 8 otros tratamientos en áreas como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen de seguro de enfermedad, dado que éstos se mencionan en el considerando 34 de la Directiva como ejemplos para invocar el apartado 4 del artículo 8".*

Dichas previsiones comunitarias son también objeto de transposición por la LOPD.

Así, el artículo 7.6 de dicha Ley Orgánica, de acuerdo con el cual

> *"No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios siempre que dicho tratamiento de datos se realice*

por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado está física o jurídicamente incapacitado para dar su consentimiento".

Tal precepto ha sido objeto de interpretación por la jurisprudencia y así la Audiencia Nacional, en Sentencia de 31 de mayo de 2002 ha indicado que la excepción prevista en el artículo 7.6 habrá de ser interpretada restrictivamente, considerando que será preciso atender en cada caso concreto a que el tratamiento se dirija efectivamente a la prevención y el diagnóstico. En este sentido, un tratamiento para un fin distinto (en el caso analizado, el control del absentismo laboral) en que estas finalidades puedan ser consideradas "secundarias" no se encontraría amparado por lo dispuesto en la Ley Orgánica 15/1999.

Más recientemente confirma dicha estricta interpretación la Sentencia del Tribunal Supremo de 20 de octubre de 2009 que casa una anterior de la Audiencia Nacional de 24 de mayo de 2007, y de acuerdo con la cual

"En cuanto a la historia clínica, es cierto que los arts. 14 y siguientes de la Ley de Autonomía del Paciente favorecen "la máxima integración posible de la documentación clínica de cada paciente" a fin de lograr una adecuada asistencia sanitaria. Tal vez ello justifique hablar, como hace la sentencia impugnada, de un principio de unidad de la historia clínica. Dicho esto, es preciso inmediatamente señalar que esa integración de la historia clínica, tendente a evitar la dispersión de la información sanitaria sobre cada paciente, tiene como beneficiario al propio paciente. El inciso inicial del art. 16 de la Ley de Autonomía del Paciente es paladinamente claro a este respecto: "La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente." Las historias clínicas no deben tener carácter unitario, como pretende la sentencia impugnada, para facilitar su misión a las mutuas de prevención de riesgos laborales, ni menos aún a los empresarios. Ciertamente, permiten prestar una asistencia sanitaria mejor; pero esta mejora no se justifica por el ahorro de esfuerzo para terceros (personal sanitario, Administración, empresarios, etc.), sino por el bienestar del paciente. Este punto es de crucial importancia, porque la información sobre la salud de las personas forma parte del objeto protegido por el derecho fundamental a la intimidad, tal como ha aclarado, entre otras, la sentencia del Tribunal Constitucional 196/2004. De aquí que toda excepción a la confidencialidad que pesa sobre dicha información sólo pueda justificarse por el beneficio que reporte al propio paciente o, en su caso, por ineludibles y superiores exigencias de interés general debidamente ponderadas, que de ningún modo pueden consistir en un funcionamiento más ágil de las mutuas de prevención de riesgos laborales. Tan es así que el art. 18 de la Ley de Autonomía del Paciente sólo confiere el derecho de acceso a la historia clínica al paciente, no a terceros; y el sucesivo art. 19 de ese mismo texto legal obliga a establecer "un mecanismo de custodia activa y diligente de las historias clínicas.

En resumen, en esta materia rige incuestionablemente la máxima confidencialidad posible, sin que haya elemento alguno en la Ley de Prevención de Riesgos Laborales o en la Ley de Autonomía del Paciente que permitan afirmar que la comunicación de datos no consentida llevada a cabo por Fremap estaba autorizada por una ley".

Por otra parte, en el marco de la asistencia sanitaria añade el artículo 8 que "*sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad*".

En este mismo sentido, recuerda el artículo 10.5 del Reglamento de desarrollo de la Ley Orgánica 15/1999 que "*no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud*".

Por último, el artículo 11.2 f) de la Ley Orgánica establece la licitud de la cesión de determinados datos relacionados con la salud si la misma es "*necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica*".

De cuanto se lleva dicho, cabe concluir a juicio de esta Agencia que el artículo 7.3 de la LOPD establece un régimen específico para los datos de salud, de modo que su tratamiento o comunicación podrá llevarse a cabo sin consentimiento del afectado sólo en caso de que una Ley así lo prevea, debiendo quedar esta habilitación fundada en la existencia de razones de interés general.

De manera más rotunda, como hace el reciente Informe de la Agencia Española de Protección de Datos 219/2008 puede decirse que "*la aplicación del artículo 7.3 de la Ley Orgánica de Protección de Datos implica, por mor del principio de especialidad, la imposible aplicación a los datos referidos en el mismo de cualquiera de las causas legitimadoras del tratamiento previstas en el artículo 11.2 de la Ley Orgánica, quedando limitados los supuestos habilitantes del tratamiento y cesión de estos datos a los establecidos en norma especial o a aquéllos en los que la norma general se refiere expresamente a tales datos*".

En consecuencia, la Ley Orgánica 15/1999 viene a establecer una lista tasada de casos en que será posible el tratamiento de los datos relacionados con la salud, quedando el mismo limitado a los supuestos en que:

- El interesado haya prestado su consentimiento expreso para ello.
- Una norma con rango de Ley así lo prevea, por razones de interés público.
- El tratamiento sea necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, con las restricciones previstas en el artículo 7.6 de la Ley Orgánica, que deberá además ser objeto de una interpretación restrictiva, en los términos ya señalados.
- El tratamiento sea necesario para atender una urgencia vital.

- El tratamiento se lleve a cabo en el ámbito de la asistencia sanitaria respecto de los pacientes que acudan a los centros sanitarios, en los términos previstos en la legislación sectorial que resulte de aplicación.
- La comunicación de los datos sea precisa para solucionar una urgencia o para realizar los estudios epidemiológicos en los términos previstos en la legislación sectorial.

Esta normativa debe ser completada con la legislación sanitaria implicada. Por tanto, en materia de protección de los datos sanitarios, deberemos prestar la máxima atención a la LOPD y su Reglamento de desarrollo, y a la normativa sanitaria que constituyen el marco normativo básico sobre el tratamiento de los datos de salud, y que complementa las reglas contenidas en la Ley Orgánica 15/1999.

V

Entrando en el análisis del texto sometido a informe, este anteproyecto de ley persigue, tal y como se explicita en el título de la norma, la adecuación de la legislación antidopaje al Código Mundial Antidopaje, para lo que modifica un número importante de preceptos de la Ley Vasca 12/2012, de 21 de junio, contra el Dopaje en el Deporte.

Esa Ley contra el Dopaje en el deporte fue informada por esta Agencia en el procedimiento de elaboración de la misma. En dicho informe de legalidad (IL10-010) se realizaron extensas consideraciones sobre la afectación de la ley al derecho fundamental de las personas a su privacidad e intimidad, y sobre los principios y garantías que deben respetarse en el tratamiento de datos personales derivados de las previsiones que la ley contiene. Nos estamos refiriendo al principio de calidad de los datos (art. 4 LOPD); al derecho de información en su recogida (art. 5 LOPD); al consentimiento del afectado (art. 6 LOPD); al tratamiento de los datos especialmente protegidos (art. 7 LOPD); a los datos relativos a la salud (art.8LPD); al deber de secreto (art. 10 LOPD); a la comunicación o cesión de datos (art. 11 LOPD) y al acceso a los datos por cuenta de terceros (art. 12 LOPD).

Sobre estos principios regulados en la LOPD, y desarrollados en el RD 1720/2007, de 21 de diciembre, incidimos en nuestro informe anterior, al que nos remitimos, en aras de evitar inútiles reiteraciones. Ello no obstante, vista la modificación legislativa proyectada, deberemos insistir en este informe en una serie de cuestiones relevantes para la protección del derecho fundamental, especialmente vinculadas con algunos de los principios de la LOPD.

En primer lugar, resulta obligado reiterar una cuestión que a juicio de esta Agencia **no está suficientemente resuelta en la ley, o al menos, no de manera clara,** como es la **delimitación del ámbito subjetivo de aplicación del régimen de control y sanción contra el dopaje**. Del articulado de la ley, en especial de su artículo 1, apartados 5 y 6; artículo 12, apartados 1 y 9 (que ahora se modifica); artículo 21.1 (que también se modifica), y Disposición Adicional Sexta, parece que sería posible aplicar el régimen de control del dopaje a deportistas federados, a quienes participen en competiciones deportivas no federadas (deportistas con licencia escolar; con licencia universitaria o mediante inscripción); y a quienes practiquen actividades deportivas de carácter no competitivo.

Esta cuestión, como ya se apuntó en el Informe IL10-010, es de capital importancia para valorar la compatibilidad de esta ley con los derechos fundamentales de las personas a su privacidad (art. 18.4 CE) y a su intimidad (art. 18.1CE), dado que a juicio de esta Agencia, **una ley que**, al menos hipotéticamente, **permita controles de dopaje a todas las personas (niños y adultos) que practiquen deporte en Euskadi, no superaría el necesario juicio de proporcionalidad** entre la finalidad del control (garantizar el juego limpio y la prevención de la salud de quienes practican algún deporte), y el respeto de los derechos y libertades fundamentales de estas personas.

En este sentido, debe recordarse que el principio de calidad de los datos (art.4.1 LOPD), exige que únicamente se recojan y traten los datos personales que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan recabado (principio de proporcionalidad). Este principio exige también (art.4.2), que los datos objeto de tratamiento no puedan usarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos (principio de finalidad), y obliga a cancelar los datos cuando dejen de ser necesarios o pertinentes para lograr la finalidad pretendida con su recogida (artículo 4.5). Además, el principio de calidad prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos (art. 4.7 LOPD).

Debemos detenernos ahora en el **nuevo artículo 38 bis**, que el anteproyecto que informamos pretende añadir a la Ley 12/2012, de 21 de junio.

> *"Artículo 38 bis.- **Divulgación de sanciones.***
>
> *1.- La identidad de cualquier deportista o persona sancionada por la infracción de alguna norma antidopaje deberá ser divulgada públicamente por la organización antidopaje responsable de la gestión de resultados en el plazo máximo de veinte días desde la firmeza de la sanción.*
>
> *2.- La organización antidopaje deberá divulgar la naturaleza de la infracción, la modalidad deportiva, la normativa antidopaje infringida, el nombre de la persona sancionada, la sustancia o método prohibido empleado en su caso y las sanciones impuestas.*
>
> *3.- La publicación se realizará como mínimo, en el sitio web de la organización antidopaje y dejándola expuesta durante un mes o la duración de cualquier periodo de suspensión, si éste fuese superior.*
>
> *4.- La comunicación obligatoria prevista en este artículo no se realizara cuando la persona sea un menor".*

Este precepto legal contempla la divulgación en internet de las sanciones impuestas en materia de dopaje, y lo hace de manera similar al Código Mundial Antidopaje.

Este Código, es una norma que carece de carácter vinculante directo para los Estados, al ser emanada por la Agencia Mundial Antidopaje, Fundación de Derecho Privado sometida al Derecho Suizo.

Sin embargo, la Convención Internacional contra el Dopaje en el Deporte de la UNESCO, una vez ratificada por los Estados, sí goza de carácter obligatorio y alcance universal, como instrumento jurídico internacional que busca la eliminación del dopaje en el deporte, promoviendo su prevención y la lucha contra el mismo. En virtud del artículo 4.1 de la Convención de la UNESCO, aprobado en París el 18 de noviembre de 2005, y ratificado

por el Estado Español en 2006, los Estados Parte se comprometen a respetar los principios del Código Mundial Antidopaje como base de las medidas internas a adoptar en la lucha contra el dopaje, que podrán comprender medidas legislativas, reglamentos, políticas o disposiciones administrativas.

La última versión del Código Mundial Antidopaje ha entrado en vigor recientemente el 1 de enero de 2015, e introduce nuevas infracciones y nuevas sanciones. Además, al mismo tiempo que prevé mayores sanciones por conductas intencionales de dopaje, permite también la aplicación de criterios de flexibilidad para la sanción de conductas en las que concurran circunstancias específicas.

Entre los principios que proclama este Código figuran el de la confidencialidad y comunicación (art. 14 del Código). Este artículo 14 del Código Mundial Antidopaje se refiere a los principios de coordinación de los resultados antidopaje, transparencia pública y responsabilidad y respeto por el derecho a la intimidad de todos los deportistas y demás personas que pueden ser sancionadas.

Dispone el art. 14.1.5 del Código Mundial Antidopaje que las organizaciones a las que esté destinada la información referida a la infracción de las normas antidopaje no podrán revelarla más allá de las personas que deban conocerla hasta que la organización antidopaje responsable de la gestión de resultados haga una divulgación pública o se niegue a hacerla, según lo dispuesto en el art. 14.3.

Ese artículo 14.3 regula la divulgación pública de la identidad de cualquier persona acusada por una organización antidopaje de la comisión de una infracción de alguna norma antidopaje, con un alcance, como decimos, similar al que contempla el proyecto sometido a dictamen.

La divulgación de sanciones en internet es desde la perspectiva de la LOPD, una cesión o comunicación de datos, definida en su artículo 3i) como *"toda revelación de datos realizada a una persona distinta del interesado"*. Esa divulgación será conforme con la LOPD, sólo si se realiza" *para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"* (artículo 11.1 LOPD).

Sin embargo, este mismo precepto legal, excepciona del consentimiento, entre otros supuestos, cuando la cesión esté amparada en una norma con rango formal de ley (artículo 11.2 a) LOPD).

También resulta relevante destacar que la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, dispone en su artículo 15, que el acceso a información pública que contenga datos especialmente protegidos del art. 7.3 de la LOPD (entre ellos, los datos de salud), o datos relativos a la comisión de infracciones penales o administrativas que no conlleven la amonestación pública al infractor, sólo podrá autorizarse con el consentimiento expreso del afectado o si está amparado por una norma con rango de ley. Este límite resulta también aplicable a la publicidad activa a la que están obligadas las Administraciones Públicas, a tenor de lo dispuesto en el artículo 5.3 de esa Ley 19/2013.

Siendo ello así, y dado que la divulgación pretendida se contempla en un anteproyecto de norma con rango formal de ley, **la publicación en internet de las sanciones en materia antidopaje se encontraría amparada por el artículo 11.2a) de la LOPD**.

Sin embargo, no obviarse que **las medidas** tendentes a lucha contra el dopaje, también las **legislativas, deben respetar los principios básicos, garantías y las limitaciones que la propia LOPD establece para el tratamiento de determinados datos** (datos de salud, datos relativos a la comisión de infracciones penales o administrativas).

En este sentido, resulta de sumo interés traer a colación el **criterio del Grupo del artículo 29 de la Directiva 95/46/CE**, en su segundo dictamen 4/2009, sobre la Norma Internacional para la protección de la intimidad y los datos personales de la Agencia Mundial Antidopaje (AMA), y sobre otros aspectos relacionados con la intimidad en el contexto de la lucha contra el dopaje en el deporte por parte del AMA y de las organizaciones naciones antidopaje, adoptado el 6 de abril de 2009, cuando señala que "*esta publicación de los datos personales y, más aún, de datos sobre las infracciones constituye una interferencia con el derecho al respeto a la intimidad y a la protección de los datos personales. Para que esta interferencia sea válida, tiene que ser necesaria para lograr un propósito legítimo específico, lo que implica, entre otros, que tienen que haber un vínculo razonable de proporcionalidad entre las consecuencias de la medida para la persona implicada y este propósito legítimo, y que no debe existir ningún otro medio de alcanzar el mismo propósito que suponga una menor intrusión*".

En este caso, la adecuación del nuevo artículo 38 bis al principio de calidad de los datos del artículo 4 de la LOPD, plantea una serie de cuestiones que resulta obligado apuntar.

Dispone el artículo 38-bis que la identidad de cualquier persona sancionada por la norma antidopaje deberá ser divulgada públicamente en el plazo de 20 días desde la firmeza de la sanción, salvo cuando se trate de un menor. Señala además, que deberá ser objeto de publicación la naturaleza de la infracción, la modalidad deportiva, la normativa antidopaje infringida, el nombre de la persona, la sustancia o método prohibido empleado en su caso, y las sanciones impuestas.

En relación con estas previsiones contenidas en este nuevo artículo 38 bis, ha de tenerse presente que **el Anteproyecto** de Ley remitido modifica el régimen sancionador en materia de dopaje, regulado en el Capítulo III de la Ley 12/2012, para adecuarlo al Código Mundial Antidopaje, y **prevé sanciones que van desde la amonestación hasta la suspensión a perpetuidad de la licencia.**

Uno de los supuestos en que procede la amonestación es cuando el deportista teniendo justificación médica suficiente para disponer de una autorización de uso terapéutico, no la haya solicitado, o haya caducado la vigencia de la anteriormente obtenida y el control arroje un resultado analítico adverso (artículo 24. 4 de la Ley 12/2012, según redacción del anteproyecto).

En este sentido, **no se alcanza a comprender que interés público se persigue con la difusión pública de esa sanción y de la sustancia empleada por ese deportista, cuando existe justificación médica para que se le autorice su uso terapéutico**.

Por ello, y a falta de mayor justificación, **esta Agencia considera que la divulgación de esta información no superaría el juicio de proporcionalidad (artículo 4.1 LOPD),** que exigiría, en todo caso, que la difusión de esa información resulte imprescindible para el cumplimiento de la finalidad que se persigue con la misma.

Resulta obligado insistir en que **los límites al derecho fundamental no sólo deben estar fijados en ley, sino que además es necesario que obedezcan 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

Por otra parte, y por lo que se refiere al plazo durante el que los datos podrán ser objeto de publicación, dispone el anteproyecto que será de un mes o la duración de cualquier período de suspensión si este fuese mayor.

Si la responsabilidad se extingue, entre otras causas, por cumplimiento de la sanción, que impide que las normas puedan prever efecto adicional de ningún tipo para las y los deportistas que hayan cumplido su sanción (artículo 33.a) de la Ley 12/2012), entiende esta Agencia que **las sanciones ya cumplidas no pueden ser objeto de publicación. Además el principio de calidad de los datos impediría que el plazo de publicación excediese del tiempo de suspensión de la licencia que se haya impuesto al sancionado.**

En otro orden de cosas, ha de tenerse en cuenta que a tenor del artículo 7.5 LOPD "*los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras*".

Ello implica que **la publicidad de las sanciones debe llevarse a efecto exclusivamente por la administración competente para la imposición de las mismas,** y en ningún caso, por una entidad ajena a la propia Administración. En este caso, la ley proyectada, modifica el artículo 10.2 de la Ley 12/2012, de 21 de junio, para reforzar el papel de la Agencia Vasca Antidopaje, como órgano especializado encargado de desarrollar las funciones atribuidas por esa Ley a la Administración General de la Comunidad Autónoma del País Vasco, entre ellas, la potestad sancionadora (artículo 10.1 e), asumiendo la condición de organización antidopaje.

En consecuencia, el organismo encargado de la publicación de las sanciones será la Agencia Vasca Antidopaje, que es la única que podrá incluir en sus ficheros los datos referidos a la comisión de esas infracciones.

Dispone también **el anteproyecto** de ley **que la publicación se realizará, "como mínimo", en el sitio web de la organización antidopaje.** De este modo, la ley contiene una especie de habilitación en blanco para que esa organización decida cuantas vías de divulgación de las sanciones estime oportunas. A juicio de esta Agencia, **debe ser la propia Ley la que,** si se estima necesario, **determine cualquier otro medio para hacer pública una información tan sensible.**

En todo caso, **se deberá advertir en la página web** de la Agencia Vasca Antidopaje, **que internet no es una fuente accesible al público, y que la información publicada no podrá ser tratada posteriormente para fines distintos.**

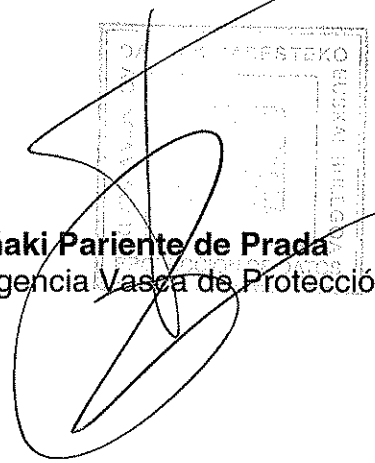
Sería también **aconsejable que la organización antidopaje adoptase las medidas oportunas para evitar la indexación de los datos publicados por los buscadores de internet,** al objeto de que la afectación al derecho fundamental sea la mínima posible.

En otro orden de cosas, y vinculado con el derecho de información en la recogida de los datos (artículo 5 LOPD), sería necesario que **en la notificación a los interesados de las resoluciones sancionadoras por dopaje, se les informe debidamente,** y con todas las

garantías exigidas por el artículo 5 de la LOPD, **que la sanción y el resto de datos** personales que contempla el artículo 38 bis, **una vez que la misma adquiera firmeza, va a ser difundida en internet y por cuanto tiempo.**

Finalmente, y en relación con el principio de seguridad de los datos, regulado en el artículo 9 de la LOPD, y en el Título VIII de su reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre, **resulta obligado que todos los laboratorios** que analicen las muestras biológicas **cumplan con las medidas de seguridad necesarias** para evitar cualquier pérdida o extravío de las mismas. En todo caso, quienes realicen tratamientos de datos por cuenta de tercero, deberán adoptar las mismas medidas de seguridad que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la LOPD.

En Vitoria-Gasteiz, a 9 de marzo de 2015



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