Informe: 0194/2017

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente al Anteproyecto de Ley Orgánica de Protección de Datos de carácter personal, solicitado de esta Agencia Española de Protección de Datos de conformidad con lo dispuesto en los artículos 37 h) de la Ley Orgánica, de 13 de diciembre, de Protección de datos de Carácter Personal, y 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 428/1993, de 26 de marzo, cúmpleme informarle lo siguiente:

I

Tal y como se desprende de su artículo 1.1, el objetivo del Anteproyecto sometido a informe es la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones (Reglamento General de Protección de Datos).

De este modo, el Anteproyecto completa el régimen regulador del derecho fundamental a la protección de datos, establecido en el mencionado Reglamento, vinculando así la aplicación del Reglamento y del propio texto a la garantía del ejercicio del derecho fundamental a la protección de datos de carácter personal, consagrado por el artículo 18.4 de la Constitución y el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea. Así, el artículo 1.2 dispone que “el derecho fundamental de las personas físicas a la protección de datos de carácter personal, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica”.

Por su parte, como indica la memoria de Análisis de Impacto Normativo “Los objetivos de la reforma proyectada deben ser examinados con relación a los siguientes aspectos:

1. Regulación del ejercicio del derecho fundamental de las personas físicas a la protección de datos de carácter personal, amparado por el artículo 18.4 de la Constitución.

2. Adaptación al Reglamento general de protección de datos para evitar contradicciones con la normativa interna y proceder a ejecutar las

previsiones del Reglamento en los puntos que el mismo Reglamento habilita.

3. Introducción de mejoras concretas en relación a aspectos del ordenamiento jurídico español en la normativa general en materia de protección de datos.

4. Introducción de mejoras concretas en relación a aspectos del ordenamiento jurídico español en las normas sectoriales en materia de protección de datos.

II

El Reglamento General de Protección de Datos se adopta con dos claros objetivos: por una parte superar la fragmentación existente en la aplicación de las normas de trasposición de la Directiva 95/46/CE, que ha dado lugar, en la práctica, y a pesar de derivar todos ellos de unos principios comúnmente aceptados, a la existencia de tantos regímenes de protección de datos como Estados Miembros, con distintos niveles de protección y, especialmente, de reacción ante conductas que pudieran suponer una infracción de la norma. Así, mientras unos ordenamientos han establecido un riguroso sistema sancionador como reacción ante supuestos de incumplimiento de estas normas, en otros sistemas el incumplimiento no ha llevado aparejada más que una advertencia o un requerimiento meramente formal al infractor, siendo incluso, en ocasiones, las competencias de investigación de las autoridades de control muy limitadas. Todo ello ha derivado en una distinta garantía del derecho y, en ocasiones, en una desventaja competitiva para entidades que llevan a cabo los mismos tratamientos atendiendo al Estado Miembro a cuyo régimen de protección de datos se encontraban sometidas.

El segundo objetivo, como indica el considerando 6 del Reglamento General de Protección de Datos, consiste en adaptar las normas de protección de datos a la rápida evolución tecnológica y a los fenómenos derivados del desarrollo exponencial de la sociedad de la información y la globalización que la misma conlleva en el tratamiento de los datos de carácter personal. Fenómenos que en 1995 eran incipientes o ni siquiera se planteaban ahora son generalmente reconocidos y forman parte del comportamiento diario de todos los operadores involucrados en la normativa de protección de datos. En efecto, el desarrollo producido en los últimos veinte años ha generado nuevas conductas en las personas titulares del derecho fundamental que forman parte sustancial de su vida cotidiana, generando al mismo tiempo nuevas situaciones de riesgo de vulneración de su derecho fundamental. Del mismo modo, los operadores responsables y encargados del tratamiento han evolucionado hacia técnicas que hace veinte años eran completamente desconocidas que, por una parte, derivan en una mayor intrusión en la privacidad y, por otra, generan

nuevos riesgos ante una quiebra en la seguridad o ante una utilización inadecuada de los datos de carácter personal.

En este ámbito el Reglamento General de Protección de Datos nace con una vocación de neutralidad tecnológica y subsistencia en el tiempo, al evolucionar desde el antiguo modelo de la Directiva 95/46/CE, que estaba basado en una serie de obligaciones a las que los responsables y encargados del tratamiento habían de sujetarse, unidas al reconocimiento de potestades reactivas de las autoridades de protección de datos, hacia un nuevo paradigma basado en lo que se denomina “enfoque de riesgo”; es decir, en la necesaria evaluación por los propios responsables y encargados del tratamiento de los riesgos que su actividad puede generar en el derecho fundamental para, a partir de esa valoración, adoptar las medidas que resulten necesarias para mitigarlos en todo lo que sea posible. Se evoluciona así hacia un modelo de responsabilidad activa, que exigirá a su vez una valoración dinámica de la actividad desarrollada por el sujeto obligado por la norma y la adopción de medidas tales como la privacidad desde el diseño y por defecto, la realización de evaluaciones de impacto en la protección de datos o la implantación de medidas de seguridad técnicas y organizativas ajustadas en cada momento al estado de la técnica y a los riesgos derivados del tratamiento. En este modelo, por otra parte, las medidas de carácter organizativo, tales como la designación de un delegado de protección de datos, sobre el que recae la función de asesorar y supervisar las actividades de tratamiento de los responsables o encargados, adquieren un papel fundamental para la salvaguarda del derecho fundamental de los afectados. Finalmente, se fomenta el establecimiento de sistemas de autorregulación, incluyendo mecanismos de resolución extrajudicial de controversias, y el desarrollo de esquemas de certificación.

Este es el marco al que los Estados miembros han de adaptar su normativa interna, partiendo de la existencia de un régimen uniforme que deberá también ser aplicado de forma uniforme en toda la Unión, aunque preservando, en lo que no contradiga ese régimen, sus principios y su tradición jurídica. Por este motivo el Reglamento General de Protección de Datos establece un buen número de habilitaciones, cuando no imposiciones, a los Estados Miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados Miembros, éstos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el Reglamento, en la medida en que sea necesario por razones de coherencia y comprensión.

Sobre estas bases se adopta el Anteproyecto ahora sometido a informe que, de acuerdo con los objetivos que se han indicado, opta por no reiterar el texto del Reglamento General de Protección de Datos para que sea asumido como integrante del derecho interno (lo que por otra parte excedería de la

habilitación establecida en el ya mencionado considerando 8, sino que intenta clarificar sus disposiciones, dentro de los márgenes que el Reglamento establece, teniendo en cuenta asimismo la propia tradición jurídica derivada de una regulación de más de veinticinco años y de una abundante doctrina judicial generada a lo largo de ese período, tanto en el ámbito interno como en el de la Unión Europea.

Por ello, como se ha indicado, junto con las previsiones destinadas a completar el contenido de los preceptos del Reglamento, el Anteproyecto incorpora determinados preceptos que, siempre dentro del ámbito del propio Reglamento, tienen por objeto clarificar la normativa que en España delimitaría el contenido esencial del derecho fundamental a la protección de datos de carácter personal, así como otras encaminadas a especificar el régimen aplicable, conforme al Reglamento, a determinados tratamientos específicos, particularmente los contenidos en el Capítulo II de su Título II

III

Dada la íntegra afectación del texto ahora objeto de informe al derecho fundamental a la protección de datos de carácter personal, el presente informe deberá, lógicamente, analizar la totalidad de su articulado, para lo que se seguirá el orden contenido en el Anteproyecto sometido a informe de esta Agencia, que, al menos en parte, se correspondería, sin perjuicio de ciertas modificaciones en la ubicación sistemática de algunos de sus Títulos o Capítulos, con lo previsto en el Reglamento General de Protección de Datos. A tal efecto, se analizará inmediatamente el Título I del Anteproyecto:

Al propio tiempo, debe tenerse en cuenta que la elaboración del texto inicial del Anteproyecto ahora sometido a informe fue encomendada por Orden del Ministro de Justicia de 2 de noviembre de 2017 a una Ponencia creada en el seno de la Sección de Derecho Público de la Comisión General de Codificación de la que formaban parte la Directora de la Agencia Española de Protección de Datos, en su condición de vocal nato de la Comisión y tres vocales adscritos, procedentes de la citada Agencia. De este modo, y sin perjuicio de las modificaciones producidas en el texto con posterioridad y durante los trámites previos a su toma en consideración por el Consejo de Ministros, la Agencia Española de Protección de Datos ha tomado parte activa en la elaboración del Anteproyecto que ahora es sometido a su informe.

Al margen de la referencia ya mencionada al objeto del Anteproyecto, el artículo 2 regula su ámbito de aplicación tratando de dar respuesta al problema derivado del distinto ámbito cubierto por las normas de protección de datos en los ámbitos internos y de la Unión Europea.

En efecto, el ámbito de una Ley nacional de protección de datos debe cubrir la totalidad de los tratamientos llevados a cabo por los sectores público y privado a menos que se establezca una norma expresa de exclusión de dicho ámbito de aplicación. En este sentido, la vigente Ley Orgánica 15/1999 enumera en su artículo 2.2 los tratamientos a los que la misma no resulta de aplicación.

Al propio tiempo, en el marco del derecho de la Unión Europea, el Reglamento general de Protección de Datos se complementa con lo establecido para determinados tratamientos por la Directiva (UE) 2016/680, del parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo

De este modo, existirán tratamientos no sujetos al derecho de la Unión que sí deban ser regulados por el derecho interno a través de la Ley general de protección de datos y, al propio interno, existirán tratamiento sí sometidos al derecho de la Unión pero que no deban regularse por esa Ley general, al encontrar su régimen amparo en otras normas de derecho de la Unión y no en el Reglamento General de Protección de Datos.

A tales efectos, el apartado 2 del artículo 2 reproduce en sus letras a) a c), como excluidos del ámbito de aplicación, aquellos tratamientos que se encuentran excluidos del ámbito del Reglamento, bien por serles de aplicación una exclusión completa de las normas de protección de datos, bien por encontrarse sometidos a la norma que trasponga la Directiva (UE) 680/2016.

Junto con estos tres supuestos, el apartado d) excluye, sin perjuicio de lo que inmediatamente se indicará, el tratamiento de datos de las personas fallecidas y el apartado e) excluye, como único supuesto expresamente excluido del ámbito de aplicación que delimita el derecho interno, las materias clasificadas.

Por su parte, el apartado 3 del precepto se refiere a aquellos tratamientos que, encontrándose sujetos al régimen interno de protección de datos no encajan en el ámbito de aplicación del Reglamento, como sucedería, por ejemplo, en relación con los ficheros electorales, los registros públicos, como el Registros Civil, el registro de la Propiedad o el registro Civil, entre otros, los tratamientos de los que sean responsables los órganos jurisdiccionales o las oficinas judiciales o los tratamientos de datos en el ámbito de la defensa nacional o de las relaciones exteriores. Respecto de los mismos, el artículo 2.3 opta por el principio de aplicación supletoria del régimen general, conformado por el Reglamento General de Protección de Datos y el propio

Anteproyecto, siendo de aplicación directa lo que se prevea en la normativa específica referida a dichos tratamientos.

De este modo, se logra integrar las normas generales de protección de datos en el sistema normativo español y, al propio tiempo, se garantizan las especialidades de dichos tratamientos, al prever la aplicación directa de su normativa específica, en términos similares a los que actualmente se derivan de lo dispuesto en el artículo 2.3 de la Ley Orgánica 15/1999.

Por su parte, el artículo 3 se refiere a los datos de las personas fallecidas, respecto de las que cabe recordar que el artículo 2.4 del Reglamento de desarrollo de la Ley Orgánica 15/1999 determina la exclusión de su ámbito de aplicación, confirmando así la postura reiteradamente manifestada por esta Agencia en el sentido de indicar que el derecho a la protección de datos es un derecho de la personalidad que, en consecuencia, se extingue por la muerte del afectado.

El considerando 27 del Reglamento general de Protección de Datos se hace eco de este principio general cuando indica, en términos luego reiterados por los considerandos 158 y 160, que “el presente Reglamento no se aplica a la protección de datos personales de personas fallecidas”.

Sin embargo, el propio considerando 27 añade que “los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas”.

El Anteproyecto hace uso de esta facultad para, a partir de lo ya previsto en el artículo 2.4 del Reglamento de desarrollo de la Ley Orgánica 15/1999, reconocer determinados derechos relacionados con estos datos. Así, Los herederos del fallecido podrán solicitar de los responsables o encargados que tratasen sus datos el acceso a los mismos, así como su rectificación o supresión. Esta previsión resulta coincidente, además, con la doctrina más reciente de la Sala de lo Contencioso-administrativo de la Audiencia nacional, plasmada en su sentencia de 3 de mayo de 2017, en la que se señala lo siguiente:

> “(…) la actora, viene a poner realmente el acento en la demanda en que ------ ha efectuado un tratamiento de los datos personales del fallecido conculcando los principios y garantías del artículo 4.4 LOPD, pues los siguió tratando, en lugar de darlos de baja, manteniéndole como tomador de una póliza de seguro de salud pese a haber fallecido, reclamando su pago y considera que dicha conducta que integra una infracción grave del artículo 44.3.c) de la LOPD y que la AEPD ha desatendido su obligación de velar por el cumplimiento de la normativa de protección de datos prevista en el artículo 37 de la LOPD, pues debía haber iniciado un expediente sancionador, lo que no ha hecho.

> Sin embargo, considera la Sala que la AEPD no ha desatendido ninguna obligación, por cuanto como razona la resolución impugnada no cabe actuación sancionadora por supuesto incumplimiento del artículo 4.4 de la LOPD en relación con el tratamiento de los datos de carácter personal de un fallecido, pese a que los mismos debieron haber sido cancelados en su día, pues como ya se ha dicho, la normativa de protección de datos deja fuera de su ámbito de aplicación dichos tratamientos. 6
>
> Cosa distinta, es que si pese a lo manifestado por ----- en el correo de 17 de abril de 2015, se persistiera en el tratamiento de los datos del fallecido pueda solicitar el recurrente a la AEPD el inicio de un procedimiento de Tutela de Derechos, que no sancionador, para la cancelación de los citados datos, lo que resulta coherente y no es contradictorio con lo sostenido en el informe jurídico 61/2008 de la AEPD."

La Ley extiende esta posibilidad también al albacea y las personas que el fallecido hubiera designado expresamente a tal efecto, así como al Ministerio fiscal en defensa de los intereses de los fallecidos menores de edad: En todo caso, mantiene intacto el ejercicio del derecho que el afectado hubiera podido llevar a cabo antes de su fallecimiento, dado que esta facultad quedará excluida cuando así lo hubiera decidido la persona fallecida, cuya voluntad debe prevalecer.

El precepto además permite que, dentro del desarrollo reglamentario previsto en el mismo, las personas puedan determinar en vida cuál consideran que ha de ser el destino adecuado de sus datos de carácter personal, siendo posible el establecimiento a través de dicha vía, en cuanto se hace referencia expresamente al registro de los mandatos e instrucciones emitidas a tal efecto a la posible regulación de Instrucciones relacionadas con los servicios de la sociedad de la información para el caso de fallecimiento.

Además, este precepto se complementa con la disposición adicional séptima del Anteproyecto, que regula el acceso a los contenidos de personas fallecidas que estuvieran siendo gestionados por los prestadores de servicios de la sociedad de la información, dejando el régimen detallado en la materia a un desarrollo reglamentario posterior.

IV

El Título II regula los principios de protección de datos, dividiéndose en dos Capítulos: el primero referido a los principios generales y el segundo a las disposiciones aplicables a tratamientos concretos. A continuación se hará referencia al primero de ellos.

El Anteproyecto adapta en el Capítulo I del Título I el derecho interno a las disposiciones del Capítulo II del Reglamento, estableciendo las especialidades que se consideran pertinentes en relación con los preceptos de dicha norma de la Unión. De este modo, los artículos 4 a 6 implicarían la adaptación al derecho español de los principios consagrados por el artículo 5 del Reglamento, los artículos 7 a 9 desarrollarían los supuestos de legitimación para el tratamiento a los que se refiere el artículo 6 del Reglamento y el artículo 10 supondría la adaptación del derecho español al artículo 9 de dicha norma.

En cuanto a los preceptos relacionados con los principios relativos al tratamiento, el artículo 4 se refiere al principio de minimización de datos, en que el Reglamento introduce en su artículo 5.1 c) una regla más restrictiva que la prevista en la Directiva, toda vez que no sólo se exige que los datos sean "adecuados, pertinentes y no excesivos" en relación con la finalidad que justifica su tratamiento, sino que se limita la tercera de las cualidades citadas, al exigir que los datos sean "limitados a los necesarios" para dichos fines.

El Anteproyecto toma en consideración esta regla, que no exige previsión alguna de adaptación, y la aplica a un supuesto específico, cual es el tratamiento de datos relacionados con la comisión de infracciones administrativas y la imposición de sanciones por dicha comisión.

En relación con tales datos, debe recordarse que el artículo 7.5 de la Ley Orgánica 15/1999 establecía restricciones específicas al tratamiento de dichos datos, considerándolos una suerte de modalidad de los datos especialmente protegidos. Dicho precepto señalaba que el tratamiento de estos datos "sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras".

A su vez, el artículo 15.1 de la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información y buen gobierno, establece, en relación con el acceso a los datos de esta naturaleza que "si la información incluyese (…) datos relativos a la comisión de infracciones (…) administrativas que no conllevasen la amonestación pública al infractor, el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley".

Esta previsión exige cohonestar el régimen regulador del tratamiento de estos datos en nuestro derecho con los principios consagrados en el Reglamento, dado que en caso de que se considerase que el tratamiento de los datos relativos a las infracciones administrativas pudiera llevarse a cabo en supuestos distintos de los previstos por el legislador para el acceso a la información pública se estaría produciendo de facto una derogación tácita de dicha Ley junto con una habilitación general para este tratamiento.

Por ello, el Anteproyecto, llevando a cabo una interpretación sistemática de los principios de protección de datos en relación con la norma que acaba de citarse viene a considerar que, dado que el acceso a datos de la naturaleza de los citados está vedado por la normativa de transparencia, cualquier tratamiento que no se funde en una de estas causas podría considerarse excesivo en relación con la finalidad en que pretendiera fundamentarse, contraviniendo el principio de minimización de los datos de carácter personal. De este modo, el artículo 4 resulta congruente tanto con el Reglamento general de Protección de Datos como con las normas que en derecho interno legitiman el acceso a información pública de estas categorías de datos de carácter personal.

Por su parte, el artículo 5 establece, respecto del principio de exactitud de los datos, consagrado por el artículo 5.1 d) del reglamento General de Protección de Datos, una aclaración similar a la ya prevista en el inciso final del artículo 8.5 del Reglamento de desarrollo de la Ley Orgánica 15/1999, según el cual “Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste”. Así, dispone el artículo 5 que “se presumirán exactos y actualizados los datos obtenidos directamente del afectado”.

Se trata con ello de evitar, en aras a la adecuada garantía de la seguridad jurídica, que pueda exigirse del responsable del tratamiento responsabilidad alguna como consecuencia del tratamiento de los datos inexactos que, deliberadamente o por error, le hubiese facilitado el afectado, así como del mantenimiento de un datos no actualizado en los supuestos en que dicho afectado se encontrase obligado a instar la actualización del dato. Por ello, ninguna observación adicional cabe efectuar respecto de dicho precepto.

Por último, el artículo 6 desarrolla lo dispuesto en el artículo 5.1 f) del reglamento, referido a los principios de seguridad y confidencialidad, adaptando a lo dispuesto en dicho reglamento el deber de secreto actualmente recogido por el artículo 10 de la Ley Orgánica 15/1999, que prácticamente se reproduce mutatis mutandi en los apartados 1 y 3 del artículo 6 del Anteproyecto.

Como única modificación respecto al régimen actualmente vigente, el precepto se limita a establecer que el deber de confidencialidad derivado de lo dispuesto en el artículo 5.1 f) del Reglamento General no debe confundirse con los deberes de secreto o confidencialidad establecidos para determinadas profesiones por otras leyes, siendo complementario de las mismas. Por este motivo, no cabe efectuar ninguna consideración adicional del precepto.

V

El resto de las disposiciones del Capítulo I del Título II del Anteproyecto se refieren a la legitimación para el tratamiento de los datos, diferenciando los artículos 7 a 9 las aplicables con carácter general y el artículo 10 las referidas a los datos especialmente protegidos.

Entrando ya en el análisis de los preceptos citados, ha de partirse con carácter previo de la directa aplicación en nuestro derecho de lo establecido en el artículo 6 del Reglamento General de Protección de Datos, cuyo apartado 1 enumera hasta seis posibles causas de legitimación para el tratamiento de datos de carácter personal.

A tal efecto, debe entenderse que el citado artículo 6.1 bien puede servir de pórtico a las previsiones contenidas en los artículos 7 a 9 del Anteproyecto, que únicamente se refieren a algunas de estas causas, como son el consentimiento y los supuestos en que el tratamiento de datos basado en el cumplimiento de una obligación legal, una misión de interés público o el ejercicio de un poder público o la existencia de un interés legítimo prevalente del responsable o de un tercero, se encuentran recogidos en una norma con rango de Ley. Sin embargo, ello no implica que el Anteproyecto limite a estos supuestos la base legal del tratamiento, sino que dichas bases procederán del citado artículo 6.1, que no es objeto de reiteración al no considerar el Anteproyecto necesario recurrir en este caso a la habilitación establecida en el considerando 8 del Reglamento General.

El artículo 7 del Anteproyecto regula el consentimiento del interesado. Para su adecuado análisis es preciso tener en cuenta cuáles eran las especialidades contenidas en el régimen actualmente vigente, así como las que establece el Reglamento, plasmadas no sólo en su artículo 7 sino en sus considerandos.

El consentimiento se configura en los artículos 6 y 11 de la Ley Orgánica 15/1999 como causa fundamental de legitimación para el tratamiento de datos de carácter personal. Dicho consentimiento, definido como declaración de voluntad libre, inequívoca, específica e informada en el artículo 3 h) de la Ley podía ser prestado, conforme al régimen que la misma y su Reglamento de desarrollo establecen, de forma explícita o “tácita o “por omisión”. A esta modalidad de consentimiento se refiere el artículo 14 del Reglamento de desarrollo de la Ley Orgánica 15/1999, que en el párrafo primero de su apartado 2 disponía que “el responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este Reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal”.

El Reglamento General de Protección de Datos define el consentimiento en su artículo 4.11 como “toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”. De este modo, resulta evidente que la obtención del consentimiento a la que se refiere el artículo 14 del Reglamento de desarrollo de la Ley Orgánica 15/1999 no resulta compatible con el régimen establecido en el Reglamento General de Protección de datos.

El considerando 32 del Reglamento aclara las disposiciones establecidas en el artículo 7 del Reglamento general, estableciendo lo siguiente:

> “El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.”

Al propio tiempo, el considerando 171 del Reglamento indica que “Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento”, por lo que a sensu contrario, si el consentimiento no encaja en el concepto ni cumple los requisitos establecidos en la definición establecida por el Reglamento, no será posible el tratamiento de los datos sobre esa única legitimación a partir de la fecha de entrada en vigor de aquél.

Consecuencia de lo anterior es la explicitación en el artículo 7.1 del Anteproyecto del concepto de consentimiento establecido por el artículo 4.11 citado, a fin de clarificar que, conforme al Reglamento General de Protección de Datos no será posible amparar un tratamiento, a partir de la fecha de su

entrada en vigor, en el consentimiento obtenido conforme al artículo 14 del Reglamento de desarrollo de la Ley Orgánica 15/1999.

En cuanto a las restantes previsiones del citado artículo 7 vendrían a clarificar cuándo cabe considerar el consentimiento como específico e inequívoco a los efectos previstos en la legislación de protección de datos, lo que exige, tal y como explica el considerando 32 ya reproducido y que es tenido en consideración en el artículo 7.2 del Anteproyecto que en caso de recabarse los datos para tratarlos en relación con distintas finalidades conste claramente el consentimiento específico para cada una de ellas.

El apartado 3 se relacionaría con el artículo 7.2 del Reglamento General, según el cual "Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento ". A tal efecto se adapta al Reglamento la previsión ya contenida en el artículo 15 del Reglamento de la Ley Orgánica 15/1999, que establece lo siguiente:

> "Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.
>
> En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento".

En cuanto al artículo 8 del Anteproyecto, referido al consentimiento para el tratamiento de datos de los menores de edad, debe recordarse que el artículo 8.1 del Reglamento general establece en principio un límite de edad de dieciséis años. No obstante, añade en su párrafo segundo que "Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años". En consecuencia, los Estados Miembros deberían determinar en su derecho interno la Ley a partir de la cual podrá prestarse el consentimiento en caso de no ser ésta la fijada en el primer párrafo del citado precepto.

El artículo 13 del Reglamento fijaba, siguiendo la doctrina de esta Agencia, la edad para esa prestación en catorce años, coincidente con la

establecida como mínimo por el Código Civil para que los menores puedan llevar a cabo actos de disposición, tales como el otorgamiento de testamento abierto.

Frente a este criterio, el Anteproyecto establece la edad de trece años; es decir, la mínima de las establecidas en el artículo 8 del Reglamento general, si bien añade una cautela que viene a exceptuar dicha regla, de modo que la misma no será de aplicación a “los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento”.

Se establece así una regla en la que, partiendo de la edad mínima prevista en el Reglamento General de protección de datos, se considera posible esta prestación, la edad podrá resultar variable en función de la actuación en cuyo contexto se solicite el consentimiento del afectado. De este modo, quedarían exceptuados todos los supuestos en los que se establece una edad superior por el legislador, bien en las normas de derecho civil o mercantil, bien en otras normativas específicas, como por ejemplo la sanitaria. Por tanto la edad de trece años únicamente sería de aplicación a los supuestos en los que, por una parte, se recabe el consentimiento del menor y, por otra, el legislador no requiera unas mayores condiciones de madurez que las que con carácter general el artículo 162.1º del Código Civil exige al menor para poder ejercer por sí mismo los derechos de la personalidad.

Por otra parte, el hecho de que esta regla se incorpore al artículo 8 determina que operará únicamente en relación con los tratamientos que se lleven a cabo sobre la base del consentimiento de los interesados. De este modo, será preciso tener en cuenta la edad del menor, que no necesariamente habrá de coincidir con la señalada en el artículo 8, en los supuestos en que dicho tratamiento no dependa exclusivamente de su voluntad, como sucederá en particular en los supuestos en que el tratamiento se fundase en la aplicación de la regla del interés legítimo preponderante, a la que se refiere el artículo 6.1 f) del reglamento general de Protección de datos, tal y como expresamente establece el inciso final de dicho precepto.

A tal efecto, debe recordarse que el considerando 38 establece cautelas sumamente claras en esta materia, al indicar que “Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño”.

El artículo 9 se refiere al tratamiento de datos amparado por una Ley, teniendo en cuenta la tradición jurídica de la normativa reguladora del derecho fundamental a la protección de datos en España, en que tanto el artículo 6.1 como el artículo 11.2 a) de la Ley Orgánica 15/1999 se refieren expresamente a la posible existencia de una habilitación legal legitimadora del tratamiento de datos de carácter personal.

Ciertamente, el artículo 6.1 del reglamento general no hace referencia a la Ley como base jurídica del tratamiento de datos, si bien en su apartado 3 clarifica que los supuestos de tratamiento de datos referidos al cumplimiento de una obligación legal o al cumplimiento de una misión de interés público o al ejercicio de una potestad pública deberán encontrarse amparados en una base legal incorporada al Derecho de la Unión o al Derecho de los Estados miembros que se aplique al responsable del tratamiento, añadiendo que:

> "La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido."

Al propio tiempo, no debe olvidarse que el artículo 8.5 del Convenio Europeo de derechos Humanos señala que "no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás". Igualmente, conforme al artículo 53.1 de la Constitución establece, en su último inciso que "Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161.1 a)".

De este modo, los apartados 1 y 2 del artículo 9 desarrollarían lo exigido por el artículo 6.3 del Reglamento General, ajustando dicha previsión al principio de reserva de Ley establecido por el citado artículo 53.1 de la Constitución.

Por su parte, el apartado 3 establece en su primer párrafo que "la ley podrá considerar fundado un determinado tratamiento en la concurrencia de un interés legítimo del responsable del tratamiento o de un tercero que prevalece sobre los derechos del afectado, en los términos previstos en el artículo 6.1 f) del Reglamento (UE) 2016/679. En estos supuestos, la ley podrá exigir al responsable la adopción garantías adicionales".

Se refiere así el Anteproyecto a los múltiples supuestos existentes en nuestro derecho en los que existe una norma con rango de Ley habilitante de un determinado tratamiento de datos que no lo impone como consecuencia de una obligación legal ni hace referencia al ejercicio de potestades de derecho público. En este sentido, debe recordarse que el artículo 10.2 a) del Reglamento de desarrollo de la Ley Orgánica 15/1999 dispone que "será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando (…) lo autorice una norma con rango de Ley o una norma de derecho comunitario y, en particular, cuando (…) el tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre".

La sentencia del Tribunal Supremo de 8 de febrero de 2012, dictada como consecuencia de la sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011 por la que se resuelve la cuestión prejudicial planteada por el Tribunal y que consideró el efecto directo del artículo 7 f) de la Directiva 85/46/CE, que se corresponde con el artículo 6.1 f) del Reglamento General, ya puso de manifiesto que el inciso que se acaba de reproducir, y que había sido objeto de impugnación por los recurrentes, no resultaba contrario al derecho español y al de la Unión Europea, expresándose del siguiente modo:

> "La razón para ello es que no se observó entonces, ni se observa ahora, confrontación entre la norma reglamentaria y la comunitaria. El que la reglamentaria establezca como excepción a la necesidad del consentimiento del interesado aquellos supuestos en que el tratamiento o la cesión están autorizados con una norma con rango de ley o una norma de derecho comunitario, ninguna adición limitativa supone con respecto a la regulación comunitaria como parece entender la recurrente.

Podría observarse una adición limitativa si se entendiera que la previsión del apartado 2 del artículo 10 exige, a falta de consentimiento del interesado, que se den los supuestos contemplados en las letras a) y b) de dicho apartado, esto es, que si no concurre la autorización de una norma con rango de ley o una norma de derecho comunitario, no está legitimado el tratamiento o cesión, aun cuando concurrieren los requisitos exigidos en el apartado b), pero como no es esa la interpretación que debe darse al precepto de mención, en cuanto claramente recoge en su apartados a) y b) dos supuestos diferenciados que por si solos legitiman el tratamiento o cesión sin necesidad del consentimiento del interesado, lejos de apreciarse un criterio restrictivo en la norma reglamentaria con respecto a la comunitaria, lo que se aprecia es la previsión en el Reglamento de un supuesto habilitador no expresamente previsto en la norma comunitaria.

También podría observarse una adición limitativa si la ley nacional habilitadora estableciera condiciones a los supuestos previstos en el artículo 7 de la Directiva, pero se comprenderá que no es ahora el momento de considerar en abstracto tal posibilidad, en todo caso siempre superable por la aplicación directa del referido artículo 7.

Lo expuesto justifica el rechazo a la impugnación del artículo 10.2 a), supuesto primero."

De este modo, el precepto no hace más que reiterar lo ya expuesto en nuestro derecho, en que se considera que, sin perjuicio de la aplicación directa de la regla de prevalencia del interés legítimo, el legislador podrá recoger supuestos en que aprecie la existencia de una presunción favorable a dicha prevalencia o considere que la misma se podría producir en caso de que el tratamiento adopte una serie de garantías adicionales. En estos supuestos, los responsables no precisarían de acudir a la regla de ponderación, dado que la Ley la habrá verificado con anterioridad. Se trata así de otorgar seguridad jurídica a los operadores, que podrán considerar de aplicación la regla de equilibrio del artículo 6.1 f) sin quedar pendientes de que la misma sea efectivamente confirmada por las autoridades de protección de datos y los órganos jurisdiccionales.

En todo caso, y siguiendo con lo señalado por el Tribunal Supremo, el Anteproyecto señala claramente que esta presunción no impedirá, en ningún supuesto "que el tratamiento de datos personales pueda considerarse lícito al amparo del artículo 6.1 f) del Reglamento (UE) 2016/679, aun cuando no exista una previsión legal específica"; es decir, cuando efectuada la ponderación deba considerarse la prevalencia del interés legítimo habilitante del tratamiento.

Finalmente, el Capítulo I del Título II se cierra con un precepto referido a los actualmente denominados datos especialmente protegidos, regulados por el artículo 9 del Reglamento General de Protección de datos.

En él se prevé, en primer lugar, la prohibición de la realización de tratamientos cuya principal finalidad sea la de revelar algunos de estos datos de carácter personal. Así se indica que "el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico".

No obstante, se indica expresamente que esta regla se aplica "a los efectos del artículo 9.2 a) del Reglamento (UE) 2016/679". Es decir, el precepto no trae causa de la prohibición general del artículo 9.1, sino del inciso final del artículo 9.2 a) del Reglamento General, según el cual el consentimiento podrá legitimar el tratamiento de datos incluidos en las categorías especiales reguladas por dicho artículo "excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado".

Se corresponde así el precepto con el artículo 7.4 de la Ley Orgánica 15/1999, a cuyo tenor "quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual". Del mismo modo en que dicha prohibición no puede levantarse actualmente por el mero hecho de que el interesado haya consentido el tratamiento, el Anteproyecto prevé que dicho tratamiento no será posible ni aun contando con el consentimiento.

Por su parte, el segundo apartado del artículo 10 se limita a clarificar la exigencia de que las normas que amparen el tratamiento de datos de salud en los supuestos establecidos en las letras g), h) e i) del artículo 9 .2 del Reglamento especifiquen las garantáis exigibles al citado tratamiento y añadan cuando corresponda, conforme exige el artículo 9.3 el deber de secreto como circunstancia que debe concurrir en quien proceda al tratamiento.

En particular, el párrafo segundo del apartado se refiere al tratamiento de datos en el ámbito de la sanidad, recogiendo lo señalado en el considerando 52 del Reglamento, según el cual:

> "Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la

legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial."

VI

El Capítulo II del Título II lleva por rúbrica "disposiciones aplicables a tratamientos concretos", estableciendo, tras una cláusula general acerca de la licitud de los tratamientos que se mencionan en el mismo, normas específicas relacionadas con determinados tratamientos de datos. De esta forma, se regulan en el propio Anteproyecto algunos supuestos en los que se prevé una legitimación específica para el tratamiento, tomando así en consideración lo establecido en el artículo 9 del propio texto, que acaba de ser analizado en el apartado anterior de este informe.

Antes de analizar las concretas disposiciones de este Capítulo procede efectuar ciertas consideraciones iniciales en cuanto al mismo:

En primer lugar, si bien la práctica totalidad de los preceptos del Capítulo se refiere a tratamientos determinados o vinculados a una determinada finalidad, estableciendo una base legal de su legitimación, es cierto que esta regla no resulta de aplicación a dos de los preceptos del Capítulo, que se refieren a la legitimación para el tratamiento de ciertas categorías de datos y no a un determinado tratamiento asociado a una finalidad concreta: son los establecidos en los artículos 12 y 20 del texto, relativos al tratamiento de datos de personas de contacto y empresarios individuales, el primero de ellos, y al tratamiento de datos de naturaleza penal, el segundo.

No obstante, incluso dentro de ambos preceptos cabe apreciar la existencia de ciertas diferencias, puesto que el primero de los mismos establece un supuesto de legitimación para el tratamiento amparado en el artículo 6.1 f) del Reglamento General de Protección de Datos, estableciendo una presunción de interés legítimo prevalente del responsable, siempre y cuando se cumplan los requisitos de la norma, entre los que se establece

expresamente la delimitación de la finalidad del tratamiento, el artículo 20 no guarda relación con el citado artículo 6.1, sino con el artículo 10 del Reglamento General, referido al tratamiento de datos relativos a condenas e infracciones penales, no estableciendo ninguna regla de ponderación ni delimitando finalidad alguna del tratamiento, sino clarificando cuándo es posible el tratamiento de estos datos.

Por este motivo, **el artículo 20 debería, a nuestro juicio, incorporarse al Capítulo I del Título II del Anteproyecto**, dado que establece las reglas generales de legitimación para el tratamiento de estos datos, cuyo carácter particularmente sensible es previsto por el artículo 10 del propio texto de la Unión. Se lograría además mantener la similitud entre la estructura del Anteproyecto y la del Reglamento General, toda vez que es al artículo 11 al que pretende adaptarse el derecho español como consecuencia de las previsiones del artículo 20.

En segundo lugar, y hecha la consideración anterior, el artículo 11 del Anteproyecto dispone como cláusula inicial del Capítulo que "Los tratamientos de datos previstos en el presente Capítulo se entenderán lícitos de acuerdo a lo establecido en el Reglamento (UE) 2016/679. Deberán respetar lo regulado en esta ley orgánica y en sus disposiciones de desarrollo".

Respecto de la primera frase del precepto, debe hacerse notar que la práctica totalidad de los preceptos del Capítulo II del Título II comienza su tenor diciendo que los citados tratamientos "serán lícitos", por lo que dicha frase no añade ninguna especialidad al régimen que se contiene con posterioridad a ella.

En cuanto a la segunda, el respeto a lo dispuesto en la Ley Orgánica y sus disposiciones de desarrollo, así como al propio Reglamento General de protección de datos no es un condicionante que deba aplicarse en especial de los tratamientos regulados por el Capítulo, dado que lógicamente, la vulneración de las disposiciones del citado Reglamento, así como de la normativa interna que adapte el ordenamiento español al mismo supondrá una vulneración de la normativa de protección de datos. Es decir, este inciso final no sólo es de aplicación a los tratamientos regulados por el Capítulo ahora analizado, sino por la totalidad de los que se lleven a cabo dentro del ámbito de aplicación del Anteproyecto.

Además, la inclusión del precepto puede inducir al error de considerar que el legislador ha entendido que sólo los tratamientos regulados por el Capítulo II del Título II pueden reputarse lícito, cuando lo cierto es que las reglas establecidas en el artículo 9 del propio Anteproyecto habilitan que otras disposiciones con rango de Ley, conforme exige el artículo 53.1 de la Constitución, puedan establecer habilitaciones legales para el tratamiento de

datos de carácter personal sobre la base de los apartados c), e) y f) del artículo 6.1 del Reglamento General de protección de datos.

De este modo, a juicio de esta Agencia, **el artículo 11 del Anteproyecto sometido a informe no aporta ninguna novedad legislativa o aclaración al contenido del texto ahora informado**.

La tercera y última consideración se refiere a la ubicación sistemática del Capítulo.

En este punto, es preciso tener en consideración la propia sistemática del texto informado en que, tras regularse por el Capítulo I del Título II los principios de protección de datos y la legitimación para el tratamiento, se regulan en el Título III los derechos de las personas recogidos en el Capítulo III del Reglamento general de protección de datos, tanto en lo referente al cumplimiento del principio de transparencia e información al interesado como en cuanto a los restantes derechos regulados por los artículo 15 a 22 del texto de la Unión Europea.

Las normas contenidas en el Capítulo II del Título II del Anteproyecto vienen a regular las particularidades de determinados tratamientos tanto en lo referente a la aplicación de los principios y la legitimación para el tratamiento como en lo que respecta al modo en que deberá cumplirse el deber de información a los interesados o, en ciertos supuestos, el modo en que se ejercitarán los derechos previstos en el Reglamento. Es decir, se establece el régimen especial de estos tratamientos tanto en relación con el Capítulo I del Título II como en lo que afecta a las disposiciones del Título III.

Sin embargo, la ubicación sistemática del Capítulo, integrado en el Título II del Anteproyecto, referido únicamente a los principios de protección de datos podría derivar en una conclusión distinta, que induciría a considerar que sus previsiones sólo son especialidades respecto del régimen general establecido en el Capítulo I de ese Título. Por ello, parece sistemáticamente preferible que las disposiciones del Capítulo ahora analizado se incorporasen al texto con posterioridad al régimen establecido en el Título III, dado que constituyen también especialidades respecto del mismo.

Tampoco la ubicación del Capítulo resulta coincidente con la del Reglamento, toda vez que no existe en realidad un Capítulo similar y, en caso de considerarse vinculado este Capítulo con el que el Reglamento General dedica a determinadas especialidades en el tratamiento de datos, su ubicación sistemática sería la del último Título del texto, siendo así que esta ubicación tampoco resultaría la óptima a juicio de esta Agencia Española de Protección de Datos.

Por todo ello, **se considera que el Capítulo II del Título II debería reubicarse, pasando a conformarse como Título IV del Anteproyecto**, de forma que le precedan las disposiciones reguladoras de los derechos de los afectados.

VII

Entrando ya en el contenido sustantivo del Capítulo II del Título II, el artículo 12 se refiere a los datos de las personas de contacto y empresarios individuales, respecto de los que se introduce una modificación sustancial en relación con el régimen actualmente aplicable.

Como es sabido, ambas categorías de datos aparecen actualmente como excluidas de la aplicación de las normas de protección de datos, en aplicación de lo establecido en los apartados 2 y 3 del Reglamento de desarrollo de la Ley Orgánica 15/1999, que dispone que:

> "2. Este Reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.
>
> 3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal."

Se establece así una ficción legal que considera que tales datos no tienen realmente el carácter de datos de carácter personal, dado que teniendo en cuenta el ámbito de aplicación establecido en el artículo 2.1 de la Ley Orgánica 15/1999, en caso contrario a la citada ficción legal, los datos se encontrarían sometidos a las normas de protección de datos.

En el régimen derivado del Reglamento General no es posible establecer tal ficción, dado que los datos a los que se refiere el artículo 12 del Anteproyecto son sin duda datos de carácter personal, referidos a personas físicas identificadas o identificables, por lo que no resulta posible mantener una exclusión como la establecida en el Reglamento de desarrollo de la Ley Orgánica.

No obstante, ciertamente, el hecho de que los datos se encuentren sometidos a la normativa de protección de datos no tiene necesariamente que

implicar que los mismos sólo puedan tratarse sobre la base del consentimiento del interesado.

En este sentido, debe recordarse que la exclusión efectuada por el Reglamento de la Ley Orgánica 15/1999 lo fue en un momento anterior a la sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, en que se declaró expresamente el efecto directo en nuestro derecho del artículo 7 f) de la Directiva 95/46/CE. Es decir, se adoptó con anterioridad a que existiese en derecho español una norma similar al citado precepto.

Dicho lo anterior, y teniendo en cuenta el efecto de la citada sentencia, parece razonable considerar que el tratamiento de datos de contacto de los empleados de una persona jurídica, cuando tenga por único objeto el mantenimiento de relaciones con la misma, así como el tratamiento de los datos de los empresarios individuales, referido exclusivamente a su actividad empresarial, es decir, a la de su establecimiento mercantil, puedan, como regla general, ampararse en el artículo 6.1 f) del Reglamento General de Protección de datos, y correlativamente en el artículo 9.3 del propio Anteproyecto.

Esta conclusión lógicamente se alcanzará en caso de que la finalidad sea la anteriormente mencionada y no el tratamiento de los datos a los que se refiere el precepto directamente referida a la propia persona de contacto o empresario individual. En este sentido ya se ha pronunciado reiteradamente esta Agencia Española de Protección de Datos al interpretar las disposiciones de los apartados 2 y 3 del artículo 2 del Reglamento de desarrollo de la Ley Orgánica 15/1999.

De este modo, procede informar favorablemente el citado artículo 12. No obstante, a fin de lograr una mayor clarificación del apartado 2 se propone clarificar la naturaleza de los datos a los que se refiere el mismo indicando lo siguiente:

> “El mismo amparo legal tendrá el tratamiento de los datos relativos a los empresarios individuales cuando se refieran a ellos **únicamente** en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.”

El artículo 13 se refiere al tratamiento de los datos hechos manifiestamente públicos por el interesado, partiendo de su licitud “siempre y cuando respete los principios establecidos en el artículo 5 del Reglamento (UE) 2016/679, se haya informado al afectado en los términos previstos en el artículo 14 del citado reglamento y se le garantice el ejercicio de sus derechos, en particular los previstos en sus artículos 17 y 19”. Además, se excluye de esta regla el tratamiento de los datos de los menores e incapacitados.

El precepto parece responder al hecho de que el Reglamento General de Protección de Datos no recoge ninguna categoría que pueda asimilarse a las tradicionalmente denominadas “fuentes accesibles al público”, definidas por el artículo 7 del Reglamento de desarrollo de la Ley Orgánica 15/1999. Ello impide establecer un régimen específico para dichas categorías de tratamientos o para el tratamiento de datos que previamente fueran objeto de tratamiento en dichas fuentes.

No obstante, el Anteproyecto toma en consideración lo señalado por el Tribunal de Justicia de la Unión Europea en la tan citada sentencia de 24 de noviembre de 2011, cuando indicaba en sus apartados 44 a 46 lo siguiente:

> “44 En lo que respecta a la ponderación requerida por el artículo 7, letra f), de la Directiva 95/46, cabe tomar en consideración el hecho de que la gravedad de la lesión de los derechos fundamentales de la persona afectada por dicho tratamiento puede variar en función de que los datos figuren ya, o no, en fuentes accesibles al público.
>
> 45 En efecto, a diferencia de los tratamientos de datos que figuran en fuentes accesibles al público, los tratamientos de datos que figuran en fuentes no accesibles al público implican necesariamente que el responsable del tratamiento y, en su caso, el tercero o terceros a quienes se comuniquen los datos dispondrán en lo sucesivo de ciertas informaciones sobre la vida privada del interesado. Esta lesión, más grave, de los derechos del interesado consagrados en los artículos 7 y 8 de la Carta debe ser apreciada en su justo valor, contrapesándola con el interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos.
>
> 46 A este respecto, procede subrayar que nada se opone a que, en ejercicio del margen de apreciación que les confiere el artículo 5 de la Directiva 95/46, los Estados miembros establezcan los principios que deben regir dicha ponderación”

De este modo, el artículo 13 ahora analizado establece un principio de presunción de prevalencia del interés legítimo del interesado cuando el interesado haya hecho, él mismo y no un tercero, manifiestamente públicos los datos de carácter general que le conciernan. En resumen, se deberá considerar que si el interesado ha permitido el libre acceso a sus datos de carácter personal por cualquier tercero, lógicamente la recogida de dichos datos, siempre y cuando se respeten las garantías mencionadas en el propio artículo 13, resulta planamente amparada en la regla del equilibrio de intereses del artículo 6.1 f) del Reglamento General de protección de datos, sin que el responsable precise de efectuar la ponderación que dicho artículo establece.

Por motivos sistemáticos se procede ahora a hacer referencia al artículo 18 del texto, dado que comparte con los dos anteriores el hecho de responder a la necesidad de adaptar el régimen actual de protección de datos a los requerimientos derivados del Reglamento general.

Según este precepto “serán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios”.

En relación con esta norma, debe recordarse que el artículo 19 del Reglamento de desarrollo de la Ley Orgánica 15/1999 establece que “en los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre”.

De este modo, el régimen actualmente vigente establece otra ficción legal aplicable a estos procesos de reestructuración societaria o de transmisión en bloque de activos y pasivos al no constar al tiempo de su aprobación la aplicación directa del artículo 7 f) de la Directiva 95/46/CE. De este modo, se convertía la comunicación de datos que efectivamente tenía lugar en una suerte de sucesión en la condición de responsable del tratamiento, al cesar en dicha situación el cedente y reemplazarle el cesionario resultante de la operación de reestructuración societaria.

Sin embargo ello generó determinados problemas, especialmente en cuanto al posible tratamiento de datos por parte de una entidad absorbente en con carácter previo a la culminación del proceso, siendo así que dicho tratamiento resultaba necesario para la efectiva culminación de la operación, garantizando su buen fin y la continuidad en la prestación de los servicios, bien por permitir la integración de los sistemas de información, bien por habilitar el cumplimiento de las obligaciones legales de la entidad resultante del proceso, por ejemplo en materia de recursos humanos. Ello dio lugar a la emisión de distintos informes de esta Agencia poniendo de manifiesto la viabilidad de ese acceso previo a los datos de carácter personal.

No cabe duda que en estos casos, o al menos en los supuestos que acaban de mencionarse, nos encontramos realmente ante una comunicación de datos de carácter personal y por ende ante un tratamiento que habrá de

fundarse en alguna de las causas de legitimación previstas en el artículo 6.1 del Reglamento General de protección de datos.

Del mismo modo, tampoco cabe duda de que, en caso de llegar a prosperar la operación de reestructuración societaria existe un interés legítimo de la entidad adquirente o resultante en continuar llevando a cabo el tratamiento de los datos de carácter personal de la entidad transmitente o preexistente, siendo así que dicho interés en un gran número de supuestos no sólo prevalecerá sobre el derecho del afectado, toda vez que la base legal del tratamiento será la que amparaba la de la preexistente, sino que a veces se llevará a cabo en el propio interés de la persona a la que se refieran los datos, manteniendo la vigencia de la relación que le unía con la entidad precedente o cedente.

VIII

El resto de los artículos contenidos en el Capítulo II del Título II se refiere a tratamientos concretos respecto de los que o bien existía con anterioridad algún tipo de previsión en la Ley Orgánica 15/1999 y sus disposiciones de desarrollo o bien estaban necesitados de una regulación específica que clarificase determinadas cuestiones relacionadas con los mismos. Entre los primeros cabe hacer referencia al régimen de los sistemas de información crediticia (artículo 14), los tratamientos con fines de videovigilancia (artículo 15) y los sistemas de exclusión publicitaria (artículo 16).

Respecto de los sistemas de información crediticia, el artículo 14 viene a recoger en el articulado del nuevo texto legal las normas ya contenidas en el artículo 29 de la Ley Orgánica 15/1999 y en sus normas de desarrollo, contenidas en el Capítulo I del Título IV de su Reglamento. Como novedad, no obstante el apartado 2 del artículo se refiere a los ficheros relacionados con el cumplimiento de obligaciones dinerarias.

Se establece así una estructura en que el apartado 1 se refiere a los tradicionalmente denominados “ficheros negativos”, respecto de los que sería de aplicación como base legitimadora del tratamiento el artículo 6.1 f) del Reglamento general de protección de datos, conforme a lo previstos en el artículo 9.3 del Anteproyecto, dedicándose el apartado 2 a los denominados “ficheros positivos”, en que el legislador considera que no procede la aplicación de la citada regla de ponderación como base legal del tratamiento, exigiendo el consentimiento del afectado. Junto con ellos, el apartado 3 establece las disposiciones comunes a ambos sistemas de información o a los sistemas en que se contengan datos tanto de cumplimientos como de incumplimientos, recogiendo las disposiciones actualmente vigentes para los ficheros de solvencia patrimonial y crédito. Finalmente, el apartado 4 establece una especialidad en lo que respecta al cumplimiento del principio de finalidad para

este tipo de sistemas de información, que no ampara la elaboración de perfiles a partir de otra información distinta.

La primera de las novedades del precepto es la regulación de los supuestos de cumplimiento de obligaciones, estableciendo el principio de que la regla de ponderación del artículo 6.1 f) del Reglamento general no opera como causa legitimadora del tratamiento, que deberá contar con el consentimiento del interesado. Se hace así eco de lo señalado por el Tribunal Supremo en su sentencia de 10 de julio de 2010, que indicaba lo siguiente:

> "Aunque lo hasta aquí expuesto es motivación suficiente para el rechazo de la impugnación objeto de examen, en respuesta a la argumentación de la recurrente relativa a que el artículo 29.2 de la Ley Orgánica permite la creación de ficheros positivos sin consentimiento de los afectados, procede indicar que la afirmación de referencia es fruto de una interpretación errónea del citado artículo 29.
>
> Con el título "Prestación de servicios de información sobre solvencia patrimonial y crédito", los apartados 1 y 2 del precepto legal dicen así:
>
> " 1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.
>
> 2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley."
>
> La lectura de dichos apartados permite concluir, en una interpretación lógico-sistemática de los mismos, que el apartado 1 se está refiriendo a los ficheros positivos o de solvencia patrimonial, exigiéndose para el tratamiento de los datos su obtención de los registros y fuentes accesibles al público o de las informaciones facilitadas por el propio interesado o con su consentimiento y que el apartado 2 hace mención a los ficheros negativos o de incumplimiento, como sin dificultad se infiere, pese a la referencia al "cumplimiento o incumplimiento de las obligaciones", de que se trata de datos facilitados por el acreedor o por quien actúe por su cuenta e interés. Lo que no resulta admisible son los ficheros positivos prescindiendo del consentimiento del afectado."

Esta doctrina fue recogida por la Agencia Española de Protección de Datos en su dictamen de 18 de abril de 2012, emitido en relación con la consulta formulada por una empresa gestora de un sistema de información crediticia en que se planteaba la procedencia de considerar el tratamiento de los datos referidos a cumplimiento de obligaciones sobre la base de la prevalencia del interés legítimo. En este punto, la Agencia, recogiendo la doctrina judicial reproducida, señalaba que:

> "En consecuencia, el propio Tribunal Supremo en el proceso en que se planteaba si la regla de ponderación del interés legítimo del responsable con los derechos del interesado se encontraba dotada de efecto Directo, dejando imprejuzgados los preceptos del Reglamento de desarrollo de la Ley Orgánica 15/1999 que consideró vinculados a la decisión final del Tribunal de Justicia de la Unión Europea, no consideró necesario esperar a dicha resolución para determinar si era posible la existencia de ficheros positivos sin contar con el consentimiento del interesado, entendiendo que dicho consentimiento sería preciso en ese caso con independencia de que la Sentencia del Tribunal de Justicia declarase el efecto directo del artículo 7 f) de la Directiva.
>
> En consecuencia, esta Agencia, siguiendo el criterio sustentado por el Tribunal Supremo, no puede sino considerar que será preciso obtener el consentimiento el interesado para la inclusión de sus datos en los denominados ficheros positivos de solvencia patrimonial y crédito."

La segunda de las novedades introducidas por el precepto es el reconocimiento expreso del régimen de corresponsabilidad de las entidades acreedoras y el responsable del sistema de información crediticia a los efectos previstos en el artículo 26 del Reglamento General de Protección de Datos. En este sentido, debe recordarse que esta cuestión ya estaba recogida en el Reglamento de desarrollo de la Ley Orgánica 1571999 cuando, atendiendo a la doctrina del Tribunal Supremo que diferenciaba en estos casos la condición del responsable del fichero común y del acreedor que era responsable del tratamiento del dato concreto incorporado al sistema señalaba en su artículo 43 que:

> "1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común.
>
> 2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre."

Al propio tiempo, el precepto clarifica o actualiza determinadas previsiones contenidas en el régimen actual de estos sistemas.

De este modo, el apartado 1 b) aclara las reclamaciones que podría determinar la no inclusión del dato de un incumplimiento en el sistema, siendo preciso que dichas reclamaciones sean planteadas por el deudor y se refieran a la existencia y cuantía de la deuda, de modo que la reclamación del acreedor o cualquier otra reclamación del deudor no impediría la inclusión de datos en un sistema de información de incumplimientos.

Igualmente el apartado 3 b) adapta el contenido del artículo 29 de la Ley Orgánica 15/1999 y sus disposiciones de desarrollo a la Ley 16/2011, de 24 de junio, de contratos de crédito al consumo, cuyo artículo 14.1 dispone que "El prestamista, antes de que se celebre el contrato de crédito, deberá evaluar la solvencia del consumidor, sobre la base de una información suficiente obtenida por los medios adecuados a tal fin, entre ellos, la información facilitada por el consumidor, a solicitud del prestamista o intermediario en la concesión de crédito. Con igual finalidad, podrá consultar los ficheros de solvencia patrimonial y crédito, a los que se refiere el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en los términos y con los requisitos y garantías previstos en dicha Ley Orgánica y su normativa de desarrollo". Asimismo, se adapta lo dispuesto en el artículo 15.2 de dicha Ley, cuando establece que "si la denegación de una solicitud de crédito se basa en la consulta de un fichero, el prestamista deberá informar al consumidor inmediata y gratuitamente de los resultados de dicha consulta y de los pormenores de la base de datos consultada".

Finalmente, la disposición adicional octava establece que "No se incorporarán a los sistemas de información crediticia a los que se refiere el artículo 14.1 deudas en que la cuantía del principal sea inferior a cincuenta euros", permitiendo que el Gobierno pueda modificar mediante real decreto dicha cuantía. Se trata con ello de evitar que la inclusión en estos sistemas de deudas de ínfima cuantía pueda comprometer la solvencia de los afectados, siendo varios los países de nuestro entorno que establecen una cuantía mínima de inclusión en este tipo de sistemas.

IX

El artículo 15 se refiere al tratamiento de datos con fines de videovigilancia, dando así rango legal a la habilitación que para estos tratamientos se derivaba de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos.

Debe tenerse en cuenta en este punto que la legitimación del tratamiento de este tipo de datos se ha visto claramente afectada por la Sentencia de 11 de diciembre de 2014 (Asunto C-212/13, František Ryneš y Úřad pro ochranu osobních údajů), referida a un supuesto de instalación por un particular, que había sido víctima de varios delitos contra la integridad de su vivienda, de un sistema de videovigilancia que no sólo grababa la entrada de su casa, sino también una porción de vía pública circundante con la misma, así como la puerta de entrada de la vivienda ubicada enfrente de la del interesado. Se planteaba si dicho sistema podía considerarse excluido de la normativa de protección de datos de carácter personal, conforme a lo previsto en el artículo 3.2 de la Directiva 95/46/CE, que excluye de la misma los tratamientos de datos con fines exclusivamente personales o domésticos, siendo la conclusión del Tribunal negativa. No obstante, la sentencia igualmente valora en el parágrafo 34 la legitimación para la instalación del sistema, considerando que "la aplicación de las disposiciones de dicha Directiva permite, en su caso, tener en cuenta, con arreglo en particular a los artículos 7, letra f), 11, apartado 2, y 13, apartado 1, letras d) y g), los intereses legítimos del responsable del tratamiento de los datos, intereses que consisten concretamente, como en el litigio principal, en proteger los bienes, la salud y la vida de dicho responsable y los de su familia".

De este modo, el Tribunal señalaba la posibilidad de que el tratamiento se amparase, aun captando la vía pública, en el artículo 7 f) de la Directiva 95/46/CE, que dispone que "los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (…) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva", al considerarse que se trataba de proteger "los bienes, la salud y la vida" del responsable.

Esta cuestión es analizada con mayor detalle por el Abogado General en sus conclusiones, presentadas el 10 de julio de 2014, indicando en sus parágrafos 63 a 67 lo siguiente:

> *"63. En lo que atañe a la legitimación de un tratamiento como el controvertido en el litigio principal, considero que dicho tratamiento puede beneficiarse de la legitimación prevista en el artículo 7, letra f), de la Directiva 95/46.*
>
> *64. En efecto, el artículo 7, letra f), de la Directiva 95/46 establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo*

perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado. Ha de tenerse en cuenta que el segundo de esos requisitos exige una ponderación de los derechos e intereses en conflicto, que dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta confieren al interesado. Dicho artículo 7, letra f), de la Directiva 95/46 es a menudo la clave indispensable para examinar la legalidad del tratamiento de datos personales.

65. En el presente caso, considero que la actividad realizada por el Sr. Ryneš tiene por objeto la protección de otros derechos fundamentales propios, como el derecho de propiedad y el derecho a la vida familiar.

66. Así pues, la aplicabilidad de la Directiva 95/46 no es necesariamente desfavorable para los intereses del responsable del tratamiento de datos personales, a condición de que éstos sean efectivamente legítimos con arreglo al artículo 7, letra f), de dicha Directiva. No parece lógico afirmar que para proteger los derechos fundamentales del Sr. Ryneš no debe aplicarse una Directiva europea cuyo objeto consiste precisamente en establecer un equilibrio justo entre los derechos de este último y los derechos de otras personas físicas, a saber, aquellas afectadas por el tratamiento de datos personales.

67. La aplicabilidad de la Directiva 95/46 a dicha situación no entraña por sí misma la ilegalidad de la actividad realizada por el Sr. Ryneš. En cambio, habría que realizar la ponderación entre los derechos fundamentales aplicables en el litigio principal en el marco de la Directiva 95/46."

Del tenor de estas consideraciones y de la conclusión alcanzada por la sentencia cabe concluir, por una parte, que el tratamiento de los datos no se encontraría excluido del ámbito de aplicación de la normativa de protección de datos, y, por otra, concluirse que dicho tratamiento se encontraría legitimado por la normativa de protección de datos en cuanto el mismo pudiera ampararse en lo dispuesto en el ya citado artículo 7 f) de la Directiva 95/46/CE, para lo que sería necesario que por aquél se respetase el principio de proporcionalidad, de modo que la grabación no pudiera considerarse excesiva para los fines que la justifican.

El artículo 15 del Anteproyecto toma en consideración esta doctrina, considerando lícito el tratamiento de los datos, siempre y cuando cumpla los requisitos previstos en el precepto, que ya se recogían en la Instrucción 1/2006 de la Agencia, tales como el respeto al principio de proporcionalidad en la captación de la vía pública (apartado 2), la conservación de los datos durante un plazo limitado a un mes (apartado 3) o la información al interesado a través de un sistema de "información por capas" (apartado 4). Del mismo modo, tomando a sensu contrario la doctrina del Tribunal de Justicia de la Unión , considera que el tratamiento de datos limitado exclusivamente al interior del domicilio del interesado sí se encontraría amparado en la denominada "excepción doméstica", dejando en todo caso a salvo lo establecido en la normativa específica reguladora de determinados sistemas de videovigilancia.

El precepto, no obstante introduce tres novedades respecto del régimen actualmente previsto, la primera de las cuales es la posibilidad de captación de imágenes de la vía pública en los supuestos previstos en el párrafo segundo del artículo 15.2; es decir, cuando le tratamiento "cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte".

A tal efecto, debe recordarse que esta Agencia Española de Protección de Datos ya analizó la posibilidad de que el principio de no captación de la vía pública pudiera exceptuarse en determinados supuestos en que el interés general así lo exigiese en su informe de 17 de mayo de 2011, que consideraba lícito el tratamiento de imágenes producido como consecuencia de la instalación en las fachadas de 457 centrales telefónicas, calificadas como estratégicas/críticas y prioritarias por la entonces Comisión del Mercado de las Telecomunicaciones "al objeto de que las mismas puedan grabar imágenes de las arquetas de registro ubicadas en la vía pública, en los recintos subterráneos y en el perímetro e inmediaciones próximas a las centrales telefónicas mencionadas", con la finalidad de garantizar la seguridad e integridad de dichas arquetas de registro, dadas las consecuencias que una manipulación o destrucción de las mismas podrían producir al servicio de comunicaciones electrónicas disponible al público. Se consideró en este caso que el interés público en el mantenimiento del servicio telefónico hacía prevalecer la legitimación de este tratamiento sobre el derecho a la protección de datos de los viandantes.

En segundo lugar, se establece respecto de estos tratamientos una exención del deber de bloqueo impuesto por el artículo 29 del Anteproyecto, al que luego se hará referencia. Se minimiza así la intromisión derivada del tratamiento, dado que las imágenes sí podrán conservarse en caso de comisión de actos ilícitos, suprimiendo así la obligación de conservación de los datos, con el consiguiente coste que ello conlleva.

Finalmente, el apartado 5 del precepto se refiere a la videovigilancia en el entorno laboral, habilitando la misma como medida de control del empleado que el empleador podría adoptar al amparo del artículo 20.3 del Estatuto de los Trabajadores, siempre y cuando los empleados hayan sido adecuadamente informados acerca de esta medida. No obstante, recogiendo la más reciente doctrina emanada del Tribunal Constitucional y del Tribunal Supremo (STC 39/2016, de 3 de marzo de 2016 y sentencia de la Sala Cuarta del Tribunal Supremo de de 31 de enero de 2017 -Recurso. 3331/2015-), se añade como segundo párrafo que "en el supuesto en que las imágenes hayan captado la comisión flagrante de un acto ilícito por los trabajadores bastará haber facilitado la información a la que se refiere el apartado anterior"; es decir, la información general referida a la existencia del sistema de videovigilancia.

X

El artículo 16 del Anteproyecto se refiere a los sistemas de exclusión publicitaria, conocidos como "listas Robinson", fijando sus condiciones básicas en términos similares a los establecidos en el artículo 49 del Reglamento de desarrollo de la Ley Orgánica 15/1999.

Así, se establece en primer lugar la licitud de estos sistemas, basados no sólo en el interés legítimo de quienes los mantienen y de los terceros que pretendan llevar a cabo tratamientos de datos con fines de prospección comercial, sino en el propio derecho de los afectados que no quieren ser objeto de este tipo de tratamientos, al haber manifestado expresamente su negativa u oposición al respecto.

Dichos sistemas incluirán los datos identificativos de los afectados, debiendo esta previsión integrarse con lo previsto en el artículo 25.2 del propio Anteproyecto, según el cual "Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa". De este modo, por datos identificativos deberá entenderse no sólo el nombre de los afectados, sino también los datos relacionados con el canal respecto del que se ejerza la oposición.

Por lo demás, se mantienen las previsiones contenidas en el artículo 49 del Reglamento de desarrollo de la Ley Orgánica 15/1999, tanto en cuanto a la obligación del responsable ante el que se ejercite la oposición de informar al afectado acerca de los sistemas de exclusión existentes como en la obligación de consulta de estos sistemas por quienes pretendan realizar el tratamiento de datos con fines de publicidad y prospección comercial, a fin de garantizar los derechos de quienes se hubieran incorporado a estos sistemas de exclusión.

XI

Dentro de los tratamientos regulados por el Capítulo II del Título II del Anteproyecto resulta novedosa la regulación contenida en los artículos 18 y 19, referidos a los sistemas de información de denuncias internas en el sector privado y a los tratamientos llevados a cabo en el ámbito de la función estadística previa.

En cuanto al último de estos tratamientos, a diferencia del regulado por el artículo 18 del Anteproyecto ciertamente existe una regulación específica a la que los mismos se encuentran sometidos. No obstante, el Anteproyecto viene a resolver determinadas cuestiones relacionadas con estos tratamientos, teniendo igualmente en cuenta las previsiones establecidas en el artículo 89 del Reglamento general de protección de datos.

En particular, el artículo 19 clarifica los supuestos en los que la transmisión de datos a los órganos competentes en materia de estadística deberá considerarse derivada de una obligación legal, conforme a lo previsto en el artículo 6.1 c) del Reglamento general de protección de datos

A tal efecto, debe tenerse en cuenta que el artículo 7.2 de la Ley 12/1989, de 9 de mayo, reguladora de la Función Estadística Pública, establece que “se establecerán por Ley las estadísticas para cuya elaboración se exijan datos con carácter obligatorio”. Esta previsión fue desarrollada por la Disposición Adicional Cuarta de la Ley 4/1990, de 29 de junio, de Presupuestos Generales del Estado para 1990, cuyo apartado y), incluido por la Disposición Adicional Segunda de la Ley 13/1996, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, indica que serán de cumplimentación obligatoria “las estadísticas que formen parte del Plan Estadístico Nacional y específicamente según el artículo 45.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, aquellas cuya realización resulte obligatoria para el Estado español por exigencia de la normativa de la Unión Europea. Asimismo, las estadísticas que pudieran realizarse al amparo del artículo 8.3 de la citada Ley”.

De ello se desprende que existirá una obligación legal de comunicar datos a los órganos competentes en materia estadística en los supuestos en los que la operación para la que se recaba la información aparezca expresamente recogida en los instrumentos de planificación estadística; es decir, el Plan Nacional de Estadística, en el ámbito estatal, o los planes aprobados en todo caso por Ley por las Comunidades Autónomas, y los correspondientes programas estadísticos anuales de ámbito estatal o autonómico.

El Anteproyecto recoge expresamente esta previsión en el primer párrafo del artículo 19.2, según el cual “La comunicación de los datos a los órganos competentes en materia estadística sólo se entenderá amparada en el artículo 6.1 e) del Reglamento (UE) 2016/679 en los casos en que la estadística para la que se requiera la información venga exigida por una norma de Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos”.

Esta regla se complementa con la exclusión expresamente prevista en el artículo 11.2 de la Ley 12/1989, que establece claramente que “En todo caso, serán de aportación estrictamente voluntaria y, en consecuencia, sólo podrán recogerse previo consentimiento expreso de los interesados los datos susceptibles de revelar el origen étnico, las opiniones políticas, las convicciones religiosas o ideológicas y, en general, cuantas circunstancias puedan afectar a la intimidad personal o familiar”.

XII

El artículo 17 del Anteproyecto regula los sistemas de información de denuncias internas en el sector privado, siendo ésta una materia que no había sido objeto de regulación específica con anterioridad, sin perjuicio de la existencia de diversos dictámenes de la Agencia Española de Protección de Datos, así como del Grupo de Trabajo creado por el artículo 29 de la Directiva95/46/CE que se referían a este tipo de tratamientos.

En cuanto a la necesidad de regular dichos sistemas, debe recordarse que el artículo 31 bis del Código Penal en la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo regula el régimen de responsabilidad penal de las personas jurídicas. Así, su apartado 1 señala que “En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables:

> a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.
>
> b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión,

> vigilancia y control de su actividad atendidas las concretas circunstancias del caso."

No obstante, el apartado 2 del artículo establece una serie de condiciones acumulativas para que pueda eximirse de responsabilidad a la persona jurídica, entre los que la condición 1ª se refiere a que "el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión".

Estos sistemas deberán cumplir los requisitos establecidos en el apartado 5 del artículo 31 bis, exigiéndose en el párrafo 4º de dicho apartado que los sistemas "Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención".

La Circular 1/2016, de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del código penal efectuada por Ley Orgánica 1/2015, al analizar los requisitos establecidos en el citado artículo 31 bis.5 4ª indica en su apartado 5.3 (bajo la rúbrica "condiciones y requisitos de los modelos de organización y gestión") lo siguiente:

> "Si bien esta primera condición del apartado 2 no lo menciona expresamente, un modelo de organización y gestión, además de tener eficacia preventiva debe posibilitar la detección de conductas criminales. Lo sugiere el cuarto requisito del apartado 5, cuando impone "la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y la observancia del modelo de prevención." La existencia de unos canales de denuncia de incumplimientos internos o de actividades ilícitas de la empresa es uno de los elementos clave de los modelos de prevención. Ahora bien, para que la obligación impuesta pueda ser exigida a los empleados resulta imprescindible que la entidad cuente con una regulación protectora específica del denunciante (*whistleblower*), que permita informar sobre incumplimientos varios, facilitando la confidencialidad mediante sistemas que la garanticen en las comunicaciones (llamadas telefónicas, correos electrónicos…) sin riesgo a sufrir represalias."

Todo ello hace necesario el establecimiento de un régimen que regule los sistemas de denuncia interna de estos ilícitos en que se recojan las garantías esenciales del derecho fundamental a la protección de datos, permitiendo a las entidades el cumplimiento de los requisitos legalmente exigidos para asegurar sus exención de la responsabilidad penal.

En relación con estos sistemas, el apartado 1 del citado artículo 17 prevé que a través de los mismos podrán "ponerse en conocimiento de una entidad privada, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable".

De este modo, frente al criterio tradicionalmente sostenido por esta Agencia Española de Protección de Datos, en que se propugnaba el carácter confidencial y no anónimo de estos sistemas, se establece la posibilidad de que las denuncias sean comunicadas al sistema "incluso anónimamente". Esta previsión, no obstante, trae causa de la fundamentación jurídica de dichos sistemas, que acaba de ser descrita, por cuanto su existencia resulta vital para la posible exención de la responsabilidad penal de la persona jurídica. Por este motivo, y aun considerándose excepcional la inclusión de estos datos, cabe concluir, de conformidad con lo señalado en la Circular 1/2016 de la Fiscalía General del Estado, que estos sistemas podrán tener el mencionado carácter.

Ello no obstante exige reforzar las garantías de exactitud y acceso a la información obrante en esos sistemas. Por este motivo, el artículo 17 establece un sistema en que se determinan claramente las garantías que deberán implantarse en los mismos a fin de poder hacer ponderar a favor del interés legítimo de la entidad responsable la legitimación para el tratamiento de los datos.

De este modo, y además de ser exigible la previa información a quienes pudieran ser objeto de denuncia de la existencia de los sistemas y d la obligación de preservar la identidad del denunciante, cuando el mismo hubiera facilitado este dato, el artículo 17 impone dos exigencias adicionales:

Por una parte, el apartado 2 limita al máximo el acceso a los datos, dado que el mismo únicamente podrá llevarse a cabo por el personal que lleve a cabo las funciones de control interno y de cumplimiento de la entidad y, sólo cuando procediera la adopción de medidas disciplinarias contra un trabajador, al personal con funciones de gestión y control de recursos humanos.

Por otra, se limita la conservación de los datos en el sistema a un período de tres meses, sin que opere en este caso la obligación de bloqueo que será objeto de análisis con posterioridad. Ello no implica que en caso de que la denuncia pueda considerarse fundada y dé lugar a una concreta investigación los datos deban suprimirse de los sistemas de la entidad, sino que únicamente procederá su supresión del concreto sistema de información de denuncias internas, pasando a integrarse en los sistemas propios del órgano de cumplimiento o, en su caso, del que tenga a su cargo la gestión de recursos humanos.

Las garantías citadas permiten aplicar en favor del responsable la regla de ponderación del interés legítimo establecida en el artículo 6.1 f) del Reglamento General de Protección de datos, procediendo así informar favorablemente este artículo.

En todo caso, debe clarificarse que los sistemas descritos en el precepto únicamente se refieren a las denuncias internas formuladas en el sector privado y ninguna relación guardan con el tratamiento de las denuncias que se formulasen, cualquiera que sea su naturaleza, ante el sector público, en que el órgano administrativo receptos de las mismas habrá de estar a lo dispuesto en su normativa específica y en la Ley 39/2015, de 1 de octubre.

XIII

Por último, debe hacerse referencia al artículo 20 del Anteproyecto, referido al "tratamiento de datos de naturaleza penal".

Como ya se ha indicado, el citado precepto, a diferencia de los que integran el Capítulo II del Título II no se refiere a un supuesto concreto de tratamiento de datos vinculado a una determinada finalidad, sino al establecimiento de las reglas que legitiman el tratamiento de los datos regulados por el artículo 10 del Reglamento general de protección de datos. De este modo, a juicio de esta Agencia, el citado precepto debería incorporarse al Capítulo I del Título II del Anteproyecto, en correlación con el hecho de ser adaptación del derecho interno al citado artículo 10.

Hecha esta consideración previa, el artículo 20 del Anteproyecto se refiere a dos supuestos claramente diferenciados: por una parte, fija en su apartado 1 las reglas generales para que quepa el tratamiento de los datos referidos a infracciones penales, condenas y medidas de seguridad; por otra, regula en su apartado 2 la legitimación para la creación y mantenimiento de registros completos de este tipo de datos de carácter personal.

En cuanto al primer apartado, debe recordase que el artículo 10 del reglamento General de protección de datos establece en su primer inciso que "el tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados".

Debe recordarse en este punto que el artículo 7.5 de la Ley Orgánica 15/1999 dispone que "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". Fuera de estos supuestos, el tratamiento de datos de esta naturaleza viene exigiendo la existencia de una Ley que lo habilite, dada la especial naturaleza de estos datos.

En relación con la posibilidad de tratamiento por quienes no son titulares de la competencia a la que se refiere el artículo 7.5 de la Ley Orgánica 15/1999 cabe recordar que esta posibilidad viene siendo reconocida por esta Agencia cuando se encuentra expresamente prevista en una Ley y se funda en derechos más dignos de protección. Al propio tiempo, debe recordarse lo previsto en el artículo 15.1 de la Ley 19/2013, de 9 de diciembre, que ya ha sido objeto de análisis al hacerse referencia al artículo 4 del Anteproyecto y que legitima el acceso a estos datos en los supuestos en los que exista una norma con rango de Ley que habilite al solicitante para que el mismo tenga lugar.

Existen diversas normas con el citado rango que legitiman el acceso y tratamiento de estos datos. Así cabe hacer referencia a las reguladoras de la protección jurídica del menor y en particular al artículo 13.5 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del código Civil y de la Ley de Enjuiciamiento Civil, introducido por el artículo 1.ocho de la Ley 26/2015, de 28 de julio, según el cual "será requisito para el acceso y ejercicio a las profesiones, oficios y actividades que impliquen contacto habitual con menores, el no haber sido condenado por sentencia firme por algún delito contra la libertad e indemnidad sexual, que incluye la agresión y abuso sexual, acoso sexual, exhibicionismo y provocación sexual, prostitución y explotación sexual y corrupción de menores, así como por trata de seres humanos. A tal efecto, quien pretenda el acceso a tales profesiones, oficios o actividades deberá acreditar esta circunstancia mediante la aportación de una certificación negativa del Registro Central de delincuentes sexuales".

De este modo, la legitimación para el tratamiento de estos datos, de conformidad con el artículo 10 del Reglamento general de protección de datos sólo sería posible en los supuestos en los que exista una Ley interna o una norma de derecho de la Unión que así lo habilite.

El inciso final, del artículo 10 del Reglamento general de Protección de datos establece, por otra parte, que "solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas".

En España, la competencia para la llevanza de este registro corresponde al Ministerio de Justicia, debiendo a tal efecto tenerse en cuenta la regulación contenida en el Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia

El Anteproyecto toma en consideración esta circunstancia, especificándola en el apartado 2 del artículo 20 y atribuyendo en exclusiva la

gestión de los sistemas “en que se recoja la totalidad de los datos relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas” al Ministerio de Justicia.

Esta previsión se complementa con lo establecido en la disposición adicional sexta del Anteproyecto, según la cual “Los datos referidos a condenas e infracciones penales o medidas de seguridad conexas podrán tratarse conforme con lo establecido en el Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia”.

A la vista de todo ello, procede emitir informe favorable respecto del artículo 20 del Anteproyecto, sin perjuicio de lo ya indicado en cuanto a su ubicación sistemática.

XIV

El Título III del Anteproyecto sometido a informe regula los derechos de las personas, adaptando el ordenamiento español a lo establecido en el Capítulo III del Reglamento general de protección de datos. A tal efecto, se recogen en tres Capítulos diferenciados las normas reguladoras del derecho de las personas a ser informadas a cerca del tratamiento (el denominado principio de transparencia e información), los restantes derechos regulados en los artículo 15 a 22, que parcialmente se corresponden con los actuales derechos de acceso, rectificación, cancelación y oposición, y la obligación de bloqueo de los datos, a la que nos referiremos posteriormente.

En cuanto a la transparencia e información al interesado, aparece regulada por el artículo 21 del Anteproyecto, vinculado directamente con los artículos 13 y 14 del Reglamento General de protección de datos, resultando especialmente relevante la habilitación conferida por los apartados 2 a 4 para que la los responsables puedan establecer un sistema de “información por capas”. De este modo, en los supuestos en que el tratamiento se lleve a cabo en el marco de un servicio de la sociedad de la información, así como en los supuestos en que la Ley lo estableciese (como sucede en el supuesto de los tratamientos con fines de videovigilancia, ya analizados) o cuando lo decida la Agencia Española de Protección de Datos, la información podrá ser facilitada a través de un sistema acumulativo, en que los elementos fundamentales sean objeto de información inmediata al interesado, pudiendo contenerse los restantes en una dirección electrónica fácilmente accesible, como por ejemplo la reguladora de la política de privacidad del responsable.

Este procedimiento de información es coincidente con el que ha sido preconizado por las autoridades de protección de datos en la “guía para el cumplimiento del deber de informar”, en cuyo apartado 5 se señala lo siguiente:

> "Para hacer compatible la mayor exigencia de información que introduce el RGPD y la concisión y comprensión en la forma de presentarla, desde las Autoridades de Protección de Datos se recomienda adoptar un modelo de información por capas o niveles.
>
> El enfoque de información multinivel consiste en lo siguiente:
>
> - presentar una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos,
>
> - remitir a la información adicional en un segundo nivel, donde se presentarán detalladamente el resto de las informaciones, en un medio más adecuado para su presentación, comprensión y, si se desea, archivo.
>
> El conjunto de las informaciones requeridas por el RGPD pueden agruparse en unos determinados epígrafes, a los efectos de su organización y presentación, especialmente en cuanto a la información a presentar, de forma resumida, en la primera capa o nivel."

En cuanto a los elementos esenciales que serán incorporados a la primera capa de información, los mismos resultan coincidentes con los mencionados en la citada guía, siendo los esenciales para que el interesado pueda conocer el alcance del tratamiento de sus datos de carácter personal y el modo en que podrá ejercer sus derechos.

XV

El Capítulo II del Título III del Anteproyecto regula los derechos reconocidos por los artículos 15 a 22 del Reglamento General de protección de datos. Gran parte de sus disposiciones contienen, en lo esencial, una remisión al régimen regulador de estos derechos contenido en el citado Reglamento. No obstante, existen determinados preceptos que introducen especialidades que deben ser particularmente tenidas en cuenta.

Así, el artículo 22 establece las reglas generales de ejercicio de estos derechos, reflejando previsiones que ya aparecen recogidas en las normas vigentes en materia de protección de datos de carácter personal.

Así, en primer lugar, se prevé que el ejercicio de los derechos podrá llevarse a cabo por el propio interesado o su representante, legal o voluntario. A tal efecto, es preciso recordar que el artículo 23 del Reglamento de desarrollo de la Ley Orgánica 15/1999, tras indicar en su apartado 1 el carácter

personalísimo de estos derechos, prevé expresamente la posibilidad de su ejercicio a través de representante legal o voluntario, recogiendo lo que esta Agencia Española de Protección de Datos ha venido apreciando de un modo invariable desde la aprobación de la Ley Orgánica 15/1999.

Del mismo modo, el Anteproyecto recoge las reglas ya contenidas actualmente en el artículo 26 del Reglamento de desarrollo de la Ley Orgánica en lo que se refiere a la posibilidad de que los derechos puedan ser objeto de atención por un encargado del tratamiento, siempre que esta circunstancia estuviese expresamente prevista en el contrato exigido por el artículo 28.3 del Reglamento general de protección de datos, por cuanto el encarado precisamente llevará a cabo el tratamiento de los datos relacionado con la gestión de estas solicitudes en nombre y por cuenta del responsable; es decir, en su condición de encargado.

El apartado 3, a su vez, clarifica la obligación del responsable de poner a disposición de los afectados los medios necesarios para ejercer sus derechos, aun cuando, en términos similares a los actualmente previstos, el interesado podrá en todo caso elegir el canal a través del cual se lleve a cabo dicho ejercicio, sin que el responsable del tratamiento pueda negarse a atender el derecho por ese exclusivo motivo, tal y como esta Agencia Española de Protección de Datos ha puesto de manifiesto en numerosas resoluciones y dictámenes.

Finalmente, resulta relevante lo dispuesto en el artículo 22.6 del Anteproyecto, según el cual “cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquéllas”.

Este precepto se corresponde con el artículo 25.8 del Reglamento de desarrollo de la Ley Orgánica 15/1999, que establece que “cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas”

Se clarifica así la posible aplicación en relación con determinados tratamientos la aplicabilidad del principio de especialidad, en virtud del cual no será posible el ejercicio de todos o algunos de los derechos consagrados en la normativa de protección de datos mediante su mera invocación, sino a través de las herramientas que, en su caso, el ordenamiento pone a disposición de los interesados. Así sucederá por ejemplo en caso de que se pretenda la rectificación o cancelación de un tratamiento derivado de un determinado acto administrativo, en que no bastará el mero ejercicio del derecho, sino que procederá la previa impugnación de dicho acto y únicamente cuando aquélla fuese estimada, se procederá a la rectificación solicitada. Del mismo modo, el

ejercicio de los derechos en relación con los determinados registros, como el Civil, el Mercantil o el de la Propiedad, se someterá a su legislación específica.

XVI

Entrando ya en la regulación de cada uno de los derechos regulados por el Capítulo II del Título III, y sin perjuicio de lo ya señalado en un lugar respecto del derecho de oposición al tratamiento de datos con fines de publicidad y prospección comercial, ya mencionado al analizarse el artículo 16 del Anteproyecto, debe hacerse especial referencia a las previsiones que el texto contiene en relación con los derechos de acceso y a la portabilidad, por cuanto se introducen reglas específicas que clarifican el contenido del reglamento general de Protección de Datos y no una mera remisión a su articulado.

En cuanto al derecho de acceso, es preciso tener en cuenta lo señalado en el artículo 63 del reglamento general de protección de datos, cuando indica que:

> "Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento. Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. Este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos. No obstante, estas consideraciones no deben tener como resultado la negativa a prestar toda la información al interesado. Si trata una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud"

El Anteproyecto recoge algunas de las aclaraciones mencionadas en el citado considerando, teniendo además en cuenta que las mismas aparecen igualmente recogidas en el Reglamento de desarrollo de la Ley Orgánica 15/1999 o han sido fijadas por la jurisprudencia del Tribunal Supremo.

Así, tal y como indica el último inciso del considerando, y teniendo en cuenta igualmente lo que ya prevé el párrafo segundo del artículo 27.2 del Reglamento de desarrollo de la Ley Orgánica, el responsable que trate una gran cantidad de información relativa al afectado que ejercite su derecho de acceso sin especificar a qué informaciones se refiere "podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud".

En cuanto a la posibilidad de que el derecho pueda otorgarse mediante un procedimiento por el que el interesado pueda acceder de modo remoto y permanente a la información, a la que se refiere igualmente el citado considerando 63, el Anteproyecto tiene en cuenta lo señalado por el Tribunal Supremo en sus sentencias de 26 de enero, 2 de julio y 22 de octubre de 2010 y 4 y 18 de febrero de 2011, que consideran el acceso remoto como una forma de atención del derecho que exime de dar una respuesta específica ante una solicitud concreta del afectado. Así, señala la primera de las sentencias citadas:

> "Ello no significa, sin embargo, que este motivo segundo haya de ser rechazado, pues la recurrente alega también que, aun admitiendo que el mencionado escrito contuviese una solicitud de acceso a datos personales, ésta resultaba injustificada desde el momento en que el solicitante disponía ya de la posibilidad permanente de acceso a sus datos personales por vía informática. Dado que este hecho ha de tenerse por cierto, es claro que la solicitud de acceso a los datos personales recogida en el escrito de 9 de febrero de 2004 era reiterativa, cuando no meramente retórica; y, por esta misma razón, presentar una reclamación ante la AEPD por incumplimiento del deber de permitir el acceso a los datos personales supone, sin duda alguna, un comportamiento contrario a la buena fe. No es leal reprochar a otro no haber hecho algo que, en realidad, ya ha hecho. Y justificar esta imputación en la inobservancia de formas y plazos previstos en la ley no deja de ser un abuso de los requisitos formales, algo que ha sido tradicionalmente visto como uno de los supuestos arquetípicos de vulneración del principio general de la buena fe. Es más: no se trata sólo de que el solicitante dispusiera de la posibilidad permanente de acceso a sus datos personales por vía informática, sino que en su escrito de 9 de febrero de 2004 no especificó mediante qué concreto medio de acceso quería que su derecho fuese satisfecho; y, en estas circunstancias, afirmar que se le denegó el acceso en el plazo legalmente previsto resulta sencillamente una abusiva deformación de la realidad."

Por su parte, el artículo 23.3 del Anteproyecto establece que “Cuando el afectado elija un medio distinto al que se le ofrece asumirá los riesgos y los costes desproporcionados que su elección comporte”.

Este precepto no es sino la aplicación de las reglas ya contenidas en los párrafos segundo y tercero del artículo 28.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999, según los cuales:

> “Si el responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.
>
> Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.”

Ello por cuanto, conforme a los principios de Reglamento general de protección de datos, el ejercicio del derecho no puede implicar un coste innecesario para el responsable. Del mismo modo, si el afectado solicita el acceso a los datos por un cauce menos seguro que el facilitado, por ejemplo, instando al responsable a no cifrar la información cuando éste la ponía a su disposición previo cifrado, no puede considerarse que el responsable no haya adoptado las medidas de responsabilidad activa impuestas por el Reglamento general, sino que es al interesado al que deberá imputarse la posible lesión de sus derechos derivada de la exigencia de no adoptar tales medidas.

Por último, el apartado 4 del artículo establece una regla que pretende establecer un criterio de seguridad jurídica en los supuestos de solicitudes reiteradas de ejercicio del derecho de acceso, considerándose como tal la reiteración del ejercicio en el plazo de seis meses. No obstante, el propio precepto establece una limitación a esta presunción, cual es, conforme a lo ya señalado en la Ley Orgánica 15/1999 y su Reglamento de desarrollo, la existencia de una causa legítima para el ejercicio del derecho.

En todo caso, el establecimiento de la regla contenida en el artículo 23.4 del Anteproyecto no puede ser considerada como impeditiva de la posibilidad de que el responsable atienda el derecho del afectado incluso sin apreciar justa causa o haga uso de la potestad que le confiere el artículo 12.3 del reglamento general de protección de datos, sometiendo el ejercicio al abono de un canon razonable y orientado a los costes derivados de la atención del derecho.

Como ya se indicó, el Anteproyecto también establece una clarificación en lo que respecta al derecho a la portabilidad de los datos, regulado por el artículo 20 del Reglamento General de Protección de Datos, al delimitar cuál es su alcance.

Así, se dispone en el primer inciso del apartado 2 del artículo 27 que "el derecho a la portabilidad no se extenderá a los datos que el responsable hubiere inferido a partir de aquellos a los que se refiere el apartado anterior".

A tal efecto, debe tenerse en cuenta lo señalado por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE en su documento de directrices sobre el derecho a la portabilidad, adoptado el 13 de diciembre de 2016 (documento WP242), en que se establece la distinción entre diferentes categorías de datos en atención a su origen a efectos de determinar si se encuentran cubiertas por el derecho a la portabilidad de los datos. Así, el documento señala que será posible diferenciar entre los datos facilitados por el afectado y los datos inferidos o derivados.

Mientras los datos facilitados por el interesado comprenderían los efectivamente facilitados de un modo activo por el afectado, así como los "facilitados" como consecuencia del uso del servicio, ates como los datos de historiales de búsquedas, tráfico o localización, los datos inferidos o derivados son "creados por el responsable sobre la base de los datos facilitados por el afectado", indicando que dichos datos no entrarían dentro del ámbito del derecho a la portabilidad. Así, se indica expresamente que en general, a la vista de lo previsto en el Reglamento general de Protección de Datos, "el término "facilitados por el afectado" debe ser interpretado en sentido amplio, excluyendo únicamente los datos inferidos y derivados, que incluyen datos personales generados por el prestador del servicio (por ejemplo, los resultados de la aplicación de un algoritmo). El responsable podrá excluir esos datos inferidos pero deberá incluir todos los restantes datos facilitados por el afectado a través de los medios técnicos puestos a su disposición por el responsable".

En todo caso, el Anteproyecto clarifica el alcance de la limitación contenida en su artículo 27.2, dado que añade que "en todo caso, el afectado podrá ejercer respecto de estos datos los restantes derechos enumerados en este capítulo, particularmente el derecho de acceso contemplado en el artículo 15 del Reglamento (UE) 2016/679".

Quiere ello decir que el interesado sí gozará respecto de los datos sometidos a tratamiento de la totalidad de los derechos establecidos en la normativa de protección de datos y, en particular, del derecho de acceso a los mismos, pudiendo así conocer tanto los datos facilitados como los inferidos o derivados. La limitación únicamente se refiere al derecho a exigir al responsable que dichos datos sean, conforme al artículo 20 del Reglamento general, recibidos por el afectado "en un formato estructurado, de uso común y

lectura mecánica" y transmitidos "a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado".

XVII

Finalmente, dentro de las disposiciones del Título III, el artículo 29 regula la obligación de bloqueo de los datos de carácter personal, configurando la misma como un tratamiento amparado por lo dispuesto en el artículo 6.1 c) del Reglamento general de Protección de Datos y habilitado por una norma con rango de Ley, el propio Anteproyecto, de conformidad con lo establecido en al artículo 6.3 del Reglamento general y el artículo 9.1 del propio Anteproyecto.

Dicho deber de bloqueo operará, conforme a lo dispuesto en el apartado 1 del artículo, tanto en los supuestos de ejercicio de los derechos de rectificación y supresión previstos en el Reglamento General de Protección de datos como en los supuestos en lo que deba procederse de oficio a la cancelación de los datos de carácter personal como consecuencia de la aplicación de los principios establecidos en el artículo 5 del mismo, como sucederá en el caso de que se hubiera cumplido el plazo de conservación de los datos o que el responsable apreciase que dichos datos no deben ya ser objeto de tratamiento o no debieron serlo incluso con anterioridad.

El bloqueo, ya recogido en la normativa vigente en materia de protección de datos de carácter personal, excluye el borrado material de los datos, si bien con las limitaciones que el propio artículo 29 establece.

Se trata así de garantizar la adecuada aplicación y supervisión del cumplimiento de las normas de protección de datos, de forma que sea posible la comprobación de los tratamientos que no resultasen conformes con el Reglamento General de protección de datos y el Anteproyecto ahora informado y sus disposiciones de desarrollo, que el responsable o el encargado podrían evitar aplicando en un sentido extensivo las reglas de supresión previstas en estas normas.

Por este motivo, el artículo 29.2, siguiendo el criterio sustentado por el artículo 16.3 de la Ley Orgánica 15/1999 y la definición de cancelación establecida en el artículo 5.1b) de su Reglamento de desarrollo establece el alcance de la obligación de bloqueo, al disponer que "los datos bloqueados quedarán a disposición exclusiva del tribunal, el Ministerio Fiscal u otras Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas", no siendo posible llevar a cabo ningún otro tratamiento de los datos para fines distintos de los citados, tal y como indica el artículo 29.3 del Anteproyecto.

En todo caso, el artículo 29.4 prevé la posibilidad de que las autoridades de protección de datos puedan establecer excepciones a la obligación de bloqueo en los supuestos en que se considere que el derecho de los interesados pueda quedar mejor garantizado si se produce la supresión inmediata de los datos aun no pudiendo los mismos ser accesibles por las autoridades judiciales o administrativas. El propio Anteproyecto contempla esta posibilidad en relación con los tratamientos con fines de videovigilancia y los sistemas de información de denuncias internas en el sector privado (artículos 15.3 y 17.4 del Anteproyecto.

XVIII

El Título IV del Anteproyecto desarrolla las denominadas obligaciones de responsabilidad activa establecidas en el Capítulo IV del Reglamento General de Protección de Datos, dividiéndose en cuatro Capítulos: el primero de ellos de carácter general y los tres restantes referidos al régimen del encargado del tratamiento, el delegado de protección de datos y los sistemas de autorregulación y certificación a los que se refiere el Reglamento General.

Como ya se indicó anteriormente, la mayor novedad que presenta el Reglamento General de Protección de Datos es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan, conforme al Capítulo IV del Reglamento General de Protección de Datos.

Dentro de las medidas establecidas en el Capítulo I de este Título, el artículo 30 parte de la premisa de que los responsables o encargados deberán ponderar, antes de llevar a cabo un tratamiento, los riesgos que del mismo podrían derivarse para los derechos y libertades de las personas y, en particular, para su privacidad, a fin de determinar a partir de dicho análisis las medidas técnicas y organizativas habrá de implantar y, en particular, si procede la realización de la evaluación de impacto en la protección de datos, regulada con mayor detalle por la Sección 3 del Capítulo IV del Reglamento general de Protección de Datos, así como si procede someter el tratamiento a la previa consulta a la autoridad de protección de datos, en los términos establecido en el artículo 36 del Reglamento.

Ciertamente, la evaluación del riesgo no aparece explícitamente recogida entre las medidas establecidas en el Capítulo IV del Reglamento general de Protección de datos. No obstante, su exigibilidad deriva directamente de la aplicación de lo que se denomina “enfoque basado en el riesgo”, dado que el artículo 24.1 del citado Reglamento dispone que las

medidas técnicas y organizativas que deberá implantar el responsable o encargado del tratamiento para poder demostrar la conformidad del tratamiento con el Reglamento deberán adoptarse “teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas”

A tal efecto, el considerando 75 del Reglamento general de Protección de Datos señala lo siguiente:

> “Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.”

El artículo 30.2 del Anteproyecto toma en consideración los supuestos generadores de riesgo a los que se refiere el citado considerando, estableciéndolos como elementos que pueden tenerse en cuenta a la hora de llevar a cabo esa evaluación previa necesaria para poder determinar la aplicación de las distintas medidas.

Respecto de dicho precepto únicamente debe apuntarse que la letra c) del artículo 30.2 se refiere los supuestos en que “se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 10 y 11 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas”. En este sentido, es preciso indicar que **en la ordenación actual del articulado, las referencias deberían entenderse**

realizadas a los artículos 10 y 20, sin perjuicio de que ya se ha propuesto el traslado de este último precepto al Capítulo I del Título II del Anteproyecto.

Los artículos 31 a 33 del Anteproyecto se refieren a algunas de las disposiciones de la sección 1 del Capítulo IV del Reglamento respecto de las que se considera necesario establecer determinadas previsiones para adaptar a las mismas el derecho español.

Así, el artículo 31 se refiere al régimen de corresponsabilidad, regulado por el artículo 26 del Reglamento, con el único propósito de clarificar dos cuestiones derivadas del mismo.

Así, el Reglamento General de Protección de Datos impone en dicho precepto que la relación entre los distintos intervinientes se plasme en un documento escrito que determine las responsabilidades de cada interviniente. La Ley Orgánica toma en consideración esta premisa y al mismo tiempo aclara que la existencia de ese documento escrito no puede servir en ningún supuesto de elemento suficiente para desvirtuar las verdaderas relaciones que existan entre los distintos implicados y el régimen de responsabilidad que haya de serles de aplicación.

De este modo, si bien será exigible que conste por escrito el instrumento que determine el alcance de las obligaciones, dicho documento no podrá ser óbice para que se adopten las medidas que corresponda si se concluyese que uno de los corresponsables habrá de responder ante las autoridades de protección de datos por determinados incumplimientos del Reglamento o el Anteproyecto.

Del mismo modo, el Anteproyecto prevé la posibilidad de que, sin perjuicio de la adopción del documento escrito al que se ha hecho referencia, las normas legitimadoras de un determinado tratamiento puedan establecer el régimen de responsabilidad de cada uno de los corresponsables. Un ejemplo de este tipo de previsión sería la aplicable a los sistemas de información crediticia, respecto de los cuales el Reglamento de desarrollo de la Ley Orgánica 15/1999 ya determina los extremos de los que habrán de responder quien gestione el sistema y los acreedores asociados al mismo.

El artículo 32 regula la figura del representante del responsable o encargado del tratamiento no establecido en la Unión Europea pero sometido al régimen del Reglamento General de Protección de Datos conforme a su artículo 3.2. En particular, se prevé que el representante responderá solidariamente con el responsable o encargado representado en caso de vulneración de las normas de protección de datos o en caso de que el tratamiento causase algún perjuicio a los afectados.

Debe en este punto recordarse que al no contar el responsable con un establecimiento en la Unión Europea no sería de aplicación al mismo ninguna de las normas reguladoras del procedimiento coordinado y el mecanismo de coherencia a los que se hará referencia con posterioridad, pudiendo cualquier autoridad de protección de datos dirigirse directamente al representante. El establecimiento de la responsabilidad solidaria, tanto en caso de incumplimiento como para la indemnización de los perjuicios causados a los responsables es la lógica consecuencia de la necesidad de garantizar el adecuado cumplimiento de las normas de protección de datos por el responsable representado, sin perjuicio de la repetición que pudiera, en su caso, corresponder al representante.

Finalmente, el artículo 33 del Anteproyecto regula el registro de operaciones de tratamiento. A tal efecto, el Anteproyecto establece como única aclaración que el contenido de dicho registro pueda asimilarse, en lo que sea posible, al que al amparo de la Ley Orgánica 15/1999 se incorporaba al Registro General de Protección de Datos de la Agencia Española de Protección de Datos, al permitir que el registro se lleve a cabo en torno a “conjuntos estructurados de datos”.

Asimismo, en el ámbito del sector público, se impone, en aras a garantizar la transparencia, que este registro, incorporando la base legal del tratamiento, sea público bajo la denominación de “inventario de actividades de tratamiento”. La publicación de este inventario, recogida en el artículo 33.2 del Anteproyecto reemplazaría a la obligación que el artículo 20 de la Ley Orgánica 15/1999 impone a las Administraciones Públicas de dictar una disposición de creación, modificación o supresión de sus ficheros, de modo que la publicidad en la sede del correspondiente responsable reemplaza a la que se verificaría mediante la publicación de la disposición en el Boletín Oficial del Estado o diario oficial correspondiente.

XIX

El Capítulo II del Título IV del Anteproyecto, formado únicamente por su artículo 34, regula el régimen del encargado del tratamiento, introduciendo las aclaraciones del artículo 28 del Reglamento general de protección de datos que derivan de las disposiciones actualmente vigentes. De este modo, toda vez que el citado artículo establece reglas claras acerca de aspectos tales como la responsabilidad in eligendo del responsable que acude a los servicios de un encargado, el contenido del contrato a celebrar entre responsable y encargado del tratamiento o el régimen de subcontratación de los servicios prestados por el encargado, no se establece ninguna especialidad.

Dentro de las reglas aplicables al encargado se parte del principio, ya establecido en el artículo 12.1 de la Ley Orgánica 15/1999, de que el acceso a

los datos por parte del encargado no precisará de una legitimación adicional a la que justifica el tratamiento delos mismos por el responsable, dado que dicho acceso no puede ser considerado una cesión de datos.

Igualmente, se recoge el principio ya establecido actualmente en el Reglamento de desarrollo de la Ley Orgánica 15/1999, y similar al establecido para los casos de corresponsabilidad en el tratamiento de que la existencia de un contrato formal no implica necesariamente la presencia de un encargado del tratamiento si éste no desarrolla actividades propias de esta figura. Así, no cabrá apreciar la existencia de un encargado cuando la actividad que desarrolla no supone únicamente la prestación de un servicio al responsable ni, en particular, cuando establezca en su propio nombre relaciones con los afectados. Con ello se pretenden evitar situaciones en que tras un entramado contractual puedan esconderse supuestos de tratamiento ilícito en que no quepa identificar al verdadero autor de la infracción.

Por otra parte, el apartado 3 del artículo 34 establece dos previsiones que hasta ahora recogía el Reglamento de desarrollo de la Ley Orgánica 15/1999 en su artículo 22: por una parte, al término del contrato, el encargado podrá, si así se lo indica el responsable, transmitir a un nuevo encargado los datos, sin llevar a cabo su devolución o destrucción. Ciertamente el Reglamento general no establece expresamente esta posibilidad; sin embargo no parece que la previsión pueda considerarse no amparada por el Reglamento general, dado que en determinados supuestos constituirá la única forma posible de que pueda producirse efectivamente una continuidad en el tratamiento de los datos, como sucedería, por ejemplo, en caso de que el servicio consista en el almacenamiento de los datos al carecer el responsable de capacidad suficiente para ello.

Asimismo, de conformidad con lo que también prevé el artículo 22 del Reglamento de desarrollo de la Ley Orgánica 15/1999, se permite que el encargado pueda conservar los datos, si bien debidamente bloqueados, en tanto fuese necesario para rendir cuentas de su gestión al responsable, dado que en caso contrario carecería de elementos suficientes para garantizar esa rendición de cuentas y el debido cumplimiento de la prestación contratada.

.

Finalmente, el artículo 34.5 del Anteproyecto recoge una previsión ya comúnmente aceptada y reiteradamente sostenida en diversos dictámenes de la Agencia Española de Protección de Datos, cual es que en el ámbito del sector público la designación de encargado del tratamiento podrá derivar de una norma que determine las competencias de un determinado órgano u organismo que preste sus servicios en un ámbito concreto; en estos casos, la propia norma reguladora del órgano u organismo podrá servir para atribuir la condición de encargado del tratamiento e incorporar los contenidos que resulten necesarios para delimitar su ámbito de actuación, siempre que cumpla

con los requisitos previstos en el artículo 26.3 del Reglamento General de Protección de Datos.

XX

El Capítulo III del Título IV del Anteproyecto se refiere a la figura del delegado de protección de datos, creada por la Sección 4 del Capítulo IV del Reglamento General de Protección de Datos y que se configura como una figura esencial en el nuevo marco establecido en el mismo.

A tal efecto, de lo dispuesto en el citado Capítulo se desprende que El delegado de protección de datos puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica, siguiendo en este punto las consideraciones efectuadas por el grupo de Trabajo creado por el l artículo 29 de la Directiva 95/46/CE en su documento de directrices del delegado de protección de datos, adoptado el 13 de diciembre de 2016 (documento WP243).

En este contexto, las corporaciones de derecho público o las asociaciones profesionales podrán incorporar como uno de los servicios ofrecidos a los responsables o encargados del tratamiento pertenecientes a las mismas, aquéllos que son propios del delegado de protección de datos, bien directamente, bien a través de entidades externas con las que hubieran llegado a algún tipo de acuerdo.

En cuanto a la primera de las cuestiones citadas, el artículo 37.1 del Reglamento general de protección de datos establece los supuestos en los que será obligatoria la designación de un delegado de protección de datos, añadiendo el apartado 4 que “en casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros”. De este modo, el Reglamento habilita a los Estados miembros a incrementar los supuestos de designación obligatoria de un delegado de protección de datos.

El Anteproyecto parte de no imponer ningún supuesto adicional de designación de un delegado de protección de datos, quedando la obligación de nombramiento del mismo circunscrita a los supuestos enumerados en el artículo 37.1. No obstante, y en aras a garantizar la seguridad jurídica, el artículo 35.1 del Anteproyecto enumera una serie de responsable o encargado que deberán considerarse comprendidos dentro de los supuestos previstos en el citado artículo del Reglamento. Dicha enumeración no es exhaustiva, por lo que existirán otros responsables o encargados sometidos a dicha obligación, si

bien se trata de clarificar el mayor número posible de supuestos en que se considera que determinados operadores jurídicos encajan en las categorías enumeradas por el tan citado artículo 37.1, fundamentalmente dentro de sus letras b) y c).

Ello debe entenderse, lógicamente, sin perjuicio de que cualquier otro responsable o encargado pueda designar voluntariamente un delegado de protección de datos. En todo caso, cualquier designación de delegado de protección de datos deberá comunicarse a la autoridad de protección de datos competente, manteniendo la Agencia Española de Protección de Datos una relación pública y actualizada de los mismos, accesible por cualquier persona. Ello resulta esencial a fin de garantizar que los afectados puedan tener un conocimiento real de quién se encarga dentro de la organización de velar por el cumplimiento de las normas de protección de datos de carácter personal. Al propio tiempo, la comunicación a las autoridades de control, prevista en el artículo 35, resulta completamente lógica si se tiene en cuenta que el artículo 39.1 del Reglamento establece como funciones del delegado de protección de datos “cooperar con la autoridad de control” (letra d) y “actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto (letra e).

En cuanto a los requisitos para ostentar la posición de delegado de protección de datos, el artículo 37.5 del reglamento General de Protección de Datos establece que “El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39”. EL Anteproyecto, a la luz de esta previsión, opta por no establecer unos requisitos adicionales específicos para poder ostentar esta condición de delegado de protección de datos, si bien será preciso que éste pueda demostrar su reconocida competencia en la materia. A tal efecto, los esquemas de certificación podrán permitir acreditar los conocimientos de quienes pudieran ostentar esta condición, aunque la certificación no será en ningún caso requisito imprescindible para acceder a este puesto, dado que el artículo 36 del Anteproyecto los configura como uno de los medios a través de los que podrá acreditarse la posesión de las competencias necesarias.

El artículo 37 del Anteproyecto regula igualmente la posición y las funciones del delegado de protección de datos, acudiendo a la habilitación prevista en el considerando 8 del Reglamento General de Protección de Datos para estructurar algunas de las previsiones referidas al mismo.

Así, conforme a lo previsto en el ya citado artículo 39.1 del reglamento general se recuerda que “el delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia

Española de Protección de Datos y las autoridades autonómicas de protección de datos" en el artículo 37.1.

Por otra parte, los apartados 2 y 3 del artículo 37 recogen lo previsto en los apartados 2 y 3 del artículo 38 del Reglamento general de protección de datos., según los cuales:

> "2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.
>
> 3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado."

De este modo, para el adecuado desempeño de sus atribuciones, el responsable o el encargado deberán dotar al delegado de medios materiales y personales suficientes y no podrán removerle salvo en los supuestos de dolo o negligencia grave.

Asimismo, y en correlación con el deber de secreto impuesto al delegado de protección de datos por el artículo 38.5 del Reglamento General de Protección de Datos, los responsables o encargados, no podrán oponer frente al delegado ningún tipo de obligación de secreto cuando solicite el acceso a los datos con la finalidad de ejercer las competencias atribuidas a los mismos por el artículo 39.1 del Reglamento.

Finalmente, se prevé, dentro de las funciones de asesoramiento y supervisión previstas en las letras a) y b) del artículo 39 del Reglamento General, el delegado comunicará a los órganos de administración o dirección que procedan las posibles irregularidades que detecte, así como las medidas que proponga para evitar la persistencia en aquéllas.

Por último el artículo 40 establece, dentro de las funciones de supervisión y asesoramiento del delegado de protección de datos atribuidas por el artículo 39 del Reglamento general de protección de datos, la posibilidad de que el mismo pueda atender las reclamaciones que le planteasen los afectados con carácter previo a que éstos acudan a la autoridad de protección de datos.

Igualmente, se prevé la posibilidad de que planteada una reclamación ante dicha autoridad ésta pueda consultar al delegado de protección de datos acerca de la misma con carácter previo a la tramitación de la reclamación.

En ambos casos se establecen plazos breves para la resolución de la reclamación, a fin de garantizar la más rápida indemnidad del derecho fundamental del afectado y, en todo caso, sin perjuicio de la posible tramitación de la reclamación por las autoridades de protección de datos.

Se impulsa con ello un medio para dar una resolución amistosa de reclamaciones, garantizando así la rápida satisfacción y restablecimiento del derecho fundamental.

XXI

Finalmente, el Capítulo IV del Título IV del Anteproyecto regula los mecanismos de autorregulación y certificación en materia de protección de datos de carácter personal, adaptando al derecho español lo previsto en la Sección 5 del Capítulo IV del Reglamento General de Protección de datos.

A tal efecto debe recordarse que conforme al considerando 98 del Reglamento general de protección de datos “Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento”.

En este punto, el Anteproyecto completa la regulación prevista en el Reglamento General de Protección de Datos, dado que la norma de la Unión se refiere a estos mecanismos a nivel europeo y no nacional.

Así, se prevé en el artículo 39.2 del Anteproyecto que los códigos de conducta puedan promoverse “además de por las asociaciones y organismos a los que se refiere el artículo 40.2 del Reglamento (UE) 2016/679, por empresas o grupos de empresas así como por los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica”. De este modo, se prevé la existencia de sistemas de autorregulación de ámbito local y por tanto más limitado que el previsto en el artículo 40 del Reglamento General de Protección de Datos.

Además, el artículo 39.3 contempla la posibilidad de que los modelos de autorregulación sean promovidos “por organismos o entidades que asuman funciones de supervisión y resolución extrajudicial de conflictos”, a los que se refiere el artículo 41 del Reglamento General de Protección de Datos.

Se pretende con ello, nuevamente, la utilización de los procedimientos y herramientas que ofrece el Reglamento General de Protección de Datos para la adopción de decisiones que permitan la más rápida salvaguarda del derecho a la protección de datos, en beneficio del propio interesado. En todo caso los organismos o entidades de supervisión deberán someterse a la evaluación de la autoridad de protección de datos, a fin de verificar que concurren los requisitos establecidos en el artículo 41 del Reglamento General de Protección de Datos, tal y como exige el artículo 39.4 del Anteproyecto.

Finalmente, el Anteproyecto establece un régimen de publicidad de los códigos de conducta que cumplan con los requisitos legalmente exigidos, sometiéndose su aprobación, en su caso al dictamen del Comité Europeo de Protección de Datos.

Estas normas se completan con la disposición transitoria segunda, referida a los códigos de conducta que con la denominación de “códigos tipo” contenida en el artículo 32 de la Ley Orgánica 15/1999 se encontrasen inscritos en la Agencia Española de Protección de Datos.

Dichos códigos, cuyo régimen no se ajusta al establecido en el Reglamento general de protección de datos “deberán adaptar su contenido a lo dispuesto en el artículo 40 del Reglamento (UE) 2016/679 en el plazo de un año a contar desde la entrada en vigor de esta ley orgánica”, procediéndose a la cancelación de la inscripción de los mismos “si, transcurrido dicho plazo, no se hubiera solicitado la autorización prevista en el artículo 39.4”.

Finalmente, respecto de los esquemas de certificación de responsables o encargados, la Ley Orgánica opta, entre los distintos modelos planteados y habilitados por los artículos 42 y 43 del Reglamento General de Protección de Datos, por atribuir a la entidad Nacional de Acreditación (ENAC) la función de acreditar a las entidades de certificación en los supuestos en que la competencia corresponda a la Agencia Española de Protección de Datos, dando aquélla cuenta a la misma de las concesiones, denegaciones o revocaciones de las acreditaciones otorgadas.

XXII

EL Título V del Anteproyecto regula las transferencias internacionales de datos, limitándose a especificar los supuestos en que será precisa la intervención de la autoridad de protección de datos de carácter personal.

No obstante, el artículo 41 del Anteproyecto sirve de pórtico a este título estableciendo un principio tradicionalmente contenido en las normas de protección de datos, cual es el de “reserva de las restantes disposiciones de protección de datos”, al que se refiere el artículo 44.1 del reglamento general.

En este sentido, el artículo 65 del reglamento de desarrollo de la Ley Orgánica 15/1999 ya disponía que “La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento”.

Esta norma es clarificada igualmente por el Anteproyecto, indicando que “En todo caso se aplicarán a los tratamientos que deriven de la propia transferencia las restantes disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos”.

Hecha esta primera precisión, el Anteproyecto diferencia los supuestos en que una transferencia internacional deberá ser objeto de aprobación por la Agencia Española de Protección de Datos, aquéllos en que procederá su autorización previa y los supuestos en que la Agencia deberá ser informada acerca de la transferencia.

De este modo, el propósito del Anteproyecto es la sistematización de los supuestos en los que es precisa la intervención de la Agencia Española de Protección de Datos para considerar una determinada transferencia internacional ajustada al régimen previsto en el Reglamento General de Protección de Datos. Es decir, no se introduce ninguna novedad frente al régimen del Reglamento general, sino que se estructura el mismo para una mejor comprensión de sus normas desde la perspectiva del derecho interno.

En cuanto a los supuestos de aprobación por la Agencia, previstos en el artículo 42 del Anteproyecto, responden a los incluidos en los artículos 46.2 d) y 47.1 del Reglamento general de Protección de Datos.

Conforme al primero de ellos, tras indicarse que las garantías adecuadas podrán ser aportadas, sin autorización de una autoridad de control, por “cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2”, añade la posibilidad de que dichas cláusulas tipo de protección de datos puedan ser “adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2”.

De este modo, la Agencia Española de Protección de Datos podrá, siempre con respeto al procedimiento mencionado con anterioridad aprobar un determinado modelo de cláusulas contractuales tipo para las transferencias

internacionales de datos, que podrá servir para la realización de aquéllas una vez supere el procedimiento previsto en el artículo 93.2 del Reglamento.

Debe a tal efecto recordarse que esta Agencia Española de Protección de Datos ya ha adoptado, dentro del marco actualmente vigente, modelos específicos de cláusulas contractuales, como las que permiten la realización de transferencias internacionales de datos entre encargados del tratamiento y sus subencargados.

No se trata de que un responsable solicite una autorización específica, sino de que la autoridad de protección de datos pueda elaborar y aprobar un modelo de contratación que pueda servir de fundamento a la transferencia.

Junto a este supuesto, el artículo 42.2 se refiere también a la aprobación por la Agencia de normas corporativas vinculantes, a las que se refiere el artículo 47 del reglamento general, cuyo apartado 1 prevé expresamente que la aprobación corresponderá a la autoridad de control de conformidad con el mecanismo de coherencia establecido en el artículo 63 del propio texto.

El artículo 48 se refiere a los supuestos sometidos a autorización de la Agencia Española de Protección de Datos, recogiendo los enumerados en el artículo 46.3 del Reglamento General de Protección de Datos, en cuya virtud “Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

> a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o
>
> b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

Es preciso recodar que esta Agencia ha hecho igualmente uso de estas habilitaciones dentro del régimen actualmente vigente, aprobando los modelos de cláusulas contractuales para la prestación de ciertos servicios de computación en nube, en cuanto al primero de los casos, o el modelo de cláusulas a incorporar en determinados memorandos de entendimiento, como en el ámbito de la cooperación con autoridades de terceros países en materia de auditoría de cuentas o prevención del blanqueo de capitales.

Por último, en cuanto a los supuestos de información a los que se refiere el artículo 44 del Anteproyecto, se incluyen los previstos en el último párrafo del artículo 49.1 del Reglamento, que establece que “cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las

disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales". Este precepto señala claramente que "el responsable del tratamiento informará a la autoridad de control de la transferencia".

Las normas reguladoras de las transferencias internacionales de datos se completan con lo previsto en la disposición adicional quinta del Anteproyecto, en que se establece que:

> "Cuando un afectado cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país beneficiario de una decisión de la Comisión de adecuación, en virtud del artículo 45 del Reglamento (UE) 2016/679, presente ante la Agencia Española de Protección de Datos una reclamación por considerar que el tratamiento de datos personales infringe dicha norma, aduciendo la incompatibilidad de la referida decisión con la protección del derecho fundamental a la protección de datos, esta solicitud deberá ser examinada, previa audiencia del responsable del tratamiento habilitado para la transferencia internacional.
>
> En el caso de que la Agencia Española de Protección de Datos considere fundada la reclamación, deberá solicitar de la Sala de lo contencioso-administrativo de la Audiencia Nacional autorización para declarar contraria a Derecho la transferencia internacional de datos sobre la que versa dicha reclamación. Esta autorización solamente podrá ser concedida si, previo planteamiento de cuestión prejudicial de validez en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea, la decisión de la Comisión Europea fuera declarada inválida por el Tribunal de Justicia de la Unión Europea."

Esta disposición trae causa de la doctrina emanada del Tribunal de Justicia de la Unión Europea en su sentencia de 6 de octubre de 2015 (Asunto C 362/14, Schrems), mediante la que el Tribunal anuló la Decisión de la Comisión 2000/520/CE, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

En dicha sentencia se analizaba, en resumidas cuentas, el supuesto en que una afectado reclamaba ante una autoridad de protección de datos la prohibición de que sus datos a una entidad ubicada en Estados Unidos y adherida a los principios de puerto seguro, resolviendo la autoridad de control que las imputaciones formuladas por el afectado en su reclamación “no podían ser eficazmente aducidas, ya que cualquier cuestión referida al carácter adecuado de la protección de los datos personales en Estados Unidos debía resolverse conforme a la Decisión 2000/520, en la que la Comisión había constatado que Estados Unidos garantizaba un nivel adecuado de protección”.

El párrafo 65 de la citada sentencia señala lo siguiente:

> “En el supuesto contrario, cuando esa autoridad considere fundadas las alegaciones expuestas por la persona que le haya presentado una solicitud para la protección de sus derechos y libertades frente al tratamiento de sus datos personales, la referida autoridad debe tener capacidad para comparecer en juicio, conforme al artículo 28, apartado 3, párrafo primero, tercer guion, de la Directiva 95/46, entendido a la luz del artículo 8, apartado 3, de la Carta. A ese efecto, corresponde al legislador nacional prever las vías de acción que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que éstos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de ésta.”

De este modo, la sentencia impone al legislador nacional la obligación de reconocer a las autoridades de protección de datos la legitimación activa para poder solicitar de los órganos jurisdiccionales nacionales la autorización para prohibir una determinada transferencia internacional de datos personales, incluso a Estados respecto de los que se haya declarado la existencia de un nivel adecuado de protección, si bien dicha autorización deberá precisar del planteamiento de la cuestión prejudicial al Tribunal de Justicia, toda vez que la adecuación procederá de una decisión de la Comisión Europea.

La disposición introduce este supuesto en nuestro ordenamiento exigiendo, lógicamente, que la solicitud de autorización vaya precedida de un procedimiento tramitado por la Autoridad de protección de datos en que, recibida la solicitud de un afectado, se dé audiencia previa al responsable que pretende llevar a cabo la transferencia, a fin de que sólo en caso de considerar procedente la prohibición a la vista de lo alegado por ambas partes se solicite la autorización ante la jurisdicción contencioso-administrativa. Si dicha jurisdicción considera que no procede la prohibición se limitará a resolver en este sentido; en caso contrario, planteará, según la disposición, la cuestión prejudicial al Tribunal de Justicia.

XXIII

El Anteproyecto dedica su Título VI a las autoridades de protección de datos, refiriéndose en su Capítulo I a la Agencia Española de Protección de Datos y en su Capítulo II a las autoridades de protección de datos de las Comunidades Autónomas y su relación con aquélla.

El considerando 117 del Reglamento General de Protección de Datos señala que "el establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa".

La regulación de las autoridades de protección de datos es una de las materias en que el Reglamento General de protección de datos impone a los Estados miembros la adopción de un régimen jurídico específico. Así, su artículo 54 establece lo siguiente:

> "1.Cada Estado miembro establecerá por ley todos los elementos indicados a continuación:
>
> a) el establecimiento de cada autoridad de control
>
> b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control;
>
> c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control;
>
> d) la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado;
>
> e) el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;
>
> f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el

cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.

2. El miembro o miembros y el personal de cada autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento."

Por lo que respecta al régimen de la Agencia Española de Protección de Datos, es particularmente relevante recalcar la "total independencia" con la que el Reglamento General de Protección de Datos inviste a las autoridades, conforme a las exigencias contenidas en la Carta de Derechos y Libertades Fundamentales de la Unión Europea. Este principio, que determina que la independencia excede de la meramente funcional para informar toda la actividad de las autoridades de control, deriva directamente de reiterada jurisprudencia del Tribunal de Justicia de la Unión, pudiendo así citarse las sentencias de 9 de marzo de 2010 (asunto C-518/07, Comisión v. Alemania), 16 de octubre de 2012 (asunto C-614/10, Comisión v. Austria) y 8 de abril de 2014 (asunto C-288/12, Comisión v. Hungría).

De este modo, el régimen de las autoridades de protección de datos debe, por una parte, evitar que la injerencia de los poderes públicos afecte al adecuado cumplimiento de las funciones y potestades que tienen encomendadas. Asimismo, por otra parte, la "total independencia" de las autoridades de protección de datos se materializa en la necesidad de que se dote a las mismas de los medios personales, materiales, técnicos y financieros necesarios para el cumplimiento efectivo de sus funciones, tal y como impone expresamente a los Estados miembros el artículo 52.4 del Reglamento General de Protección de Datos al disponer que "cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité".

Hecha esta consideración, no cabe duda de que la Agencia Española de Protección de Datos se encuadra necesariamente dentro de lo que la Ley 40/2015, de 1 de octubre, de Régimen jurídico del sector público, denomina "Autoridades Administrativas Independientes", quedando así sometida a su normativa específica y supletoriamente, y en cuanto sea compatible con su plena independencia, a lo establecido en las normas generales del Derecho

Administrativo. Así se prevé en el artículo 45.1, que recalca, de conformidad con el Reglamento general de Protección de Datos que la Agencia "actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones".

Asimismo, el Anteproyecto mantiene el régimen peculiar de la Agencia Española de Protección de Datos que actualmente establecen la Ley Orgánica 15/1999 y el estatuto de la Agencia, en el sentido de no prever ningún tipo de adscripción de aquélla a un concreto departamento Ministerial. De este modo, y manteniendo el régimen vigente, el artículo 45.1 del Anteproyecto dispone que la Agencia "se relaciona con el Gobierno a través del Ministerio de Justicia".

Por otra parte, el artículo 68.4 del Reglamento General de protección de datos establece que "cuando en un Estado miembro estén encargados de controlar la aplicación de las disposiciones del presente Reglamento varias autoridades de control, se nombrará a un representante común de conformidad con el Derecho de ese Estado miembro". Este mandato se cumple mediante el artículo 45.2 del Anteproyecto, que otorga esta condición a la Agencia Española de Protección de Datos, sin perjuicio de la colaboración de la misma con las restantes autoridades de control, regulada por la Sección segunda del Capítulo II del Título VI del Anteproyecto.

Por último, debe recordarse que en el ámbito del poder Judicial, el artículo 236 nonies de la Ley Orgánica del Poder Judicial delimita las competencias como autoridad de protección de datos de la propia Agencia y el Consejo General del Poder Judicial, disponiendo que, por una parte "las competencias que la Ley Orgánica 15/1999, de 13 de diciembre, atribuye a la Agencia Española de Protección de Datos, serán ejercidas, respecto de los tratamientos efectuados con fines jurisdiccionales y los ficheros de esta naturaleza, por el Consejo General del Poder Judicial" y, por otra "los tratamientos de datos llevados a cabo con fines no jurisdiccionales y sus correspondientes ficheros quedarán sometidos a la competencia de la Agencia Española de Protección de Datos, prestando el Consejo General del Poder Judicial a la misma la colaboración que al efecto precise".

Añade el apartado 3 del precepto que "cuando con ocasión de la realización de actuaciones de investigación relacionadas con la posible comisión de una infracción de la normativa de protección de datos las autoridades competentes a las que se refieren los dos apartados anteriores apreciasen la existencia de indicios que supongan la competencia de la otra autoridad, darán inmediatamente traslado a esta última a fin de que prosiga con la tramitación del procedimiento".

Estas previsiones son tenidas en cuenta por el apartado 3 del artículo 45 del Anteproyecto, al establecer que "La Agencia Española de Protección de Datos y el Consejo General del Poder Judicial colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica

6/1985, de 1 julio, del Poder Judicial, les atribuye en materia de protección de datos de carácter personal en el ámbito de la Administración de Justicia".

XXIV

En lo que respecta al régimen jurídico de la Agencia Española de Protección de Datos, el artículo 46 somete a la misma a lo dispuesto en el Reglamento General de protección de datos, el propio Anteproyecto y sus disposiciones de desarrollo.

Cabe recordar que, como se ha indicado, el artículo 110.1 de la Ley 40/2015, dispone que "Las autoridades administrativas independientes se regirán por su Ley de creación, sus estatutos y la legislación especial de los sectores económicos sometidos a su supervisión y, supletoriamente y en cuanto sea compatible con su naturaleza y autonomía, por lo dispuesto en esta Ley, en particular lo dispuesto para organismos autónomos, la Ley del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 47/2003, de 26 de noviembre, el Real Decreto Legislativo 3/2011, de 14 de noviembre, la Ley 33/2003, de 3 de noviembre, así como el resto de las normas de derecho administrativo general y especial que le sea de aplicación. En defecto de norma administrativa, se aplicará el derecho común".

En este punto resulta especialmente relevante tener en cuenta que la aplicación supletoria de estas normas de derecho administrativo únicamente podrá tener lugar en cuanto no afecte o comprometa el régimen peculiarísimo de independencia de las autoridades de protección de datos, establecido en el Reglamento general de Protección de Datos.

A tal efecto, la disposición adicional décima del Anteproyecto establece algunas peculiaridades de dicho régimen, al prever que "La Agencia Española de Protección de Datos podrá adherirse a los sistemas de contratación centralizada establecidos por las Administraciones Públicas y participar en la gestión compartida de servicios comunes".

En el mismo sentido, y aun cuando el Anteproyecto no establezca una previsión específica al respecto, debe tenerse en cuenta que esta independencia afecta asimismo a la aplicación de determinadas previsiones de la Ley 40/2015, como las referentes al régimen de control de eficacia y supervisión continua establecido en su artículo 85, o las que exigirían la previa autorización por el Ministerio de Hacienda y Función Pública de los Convenios de colaboración que aquélla firmase en el desempeño de sus competencias, conforme al artículo 50.2 c) de la misma Ley.

Respecto a la primera de las cuestiones, el dictamen del Consejo de estado de 29 de abril de 2015 señalaba claramente lo siguiente:

> “La intensidad con que tales controles se regulan en el artículo 60 del anteproyecto parece, en todo caso, difícilmente conciliable con la independencia que debe caracterizar a estas autoridades administrativas en el ejercicio de sus funciones. Adviértase que se trata de un control que alcanza a "la subsistencia de las circunstancias que justificaron su creación" y a "la concurrencia de la causa de disolución referida al incumplimiento de los fines que justificaron su creación o a que su subsistencia no resulte el medio más idóneo para lograrlos" (artículo 60.3.a) y c)). La atribución de un control de esta naturaleza al Ministerio de Hacienda y Administraciones Públicas y, en el seno de éste, a la Intervención General de la Administración del Estado, es compatible con la nota de dependencia que caracteriza a las personificaciones instrumentales, pero no lo es con la posición de aquellos organismos públicos a los que la Ley ha reconocido un estatuto de independencia en el ejercicio de sus funciones frente al Gobierno y a la Administración del Estado.
>
> No son pocas las experiencias que, en fechas no demasiado lejanas, han venido a evidenciar la importancia de que estos organismos ejerzan sus funciones de supervisión o regulación con independencia del Gobierno y de la Administración General del Estado. Dicha independencia exige que ésta no pueda ejercer controles orientados a supervisar la actuación de las autoridades administrativas independientes que, a la postre, pudieran afectar de forma directa o indirecta a la neutralidad de éstas.”

Por su parte, respecto de la autorización previa de los Convenios, el Dictamen de la Abogacía General del Estado de 11 de octubre de 2016, siguiendo la doctrina del Consejo de Estado anteriormente mencionada, indicaba que:

> “Pues bien, la necesidad de garantizar en todo caso la esfera de autonomía o independencia que para el ejercicio de sus funciones e regulación y supervisión ostentan las entidades de que se trata, la dificultad de distinguir entre convenios que, directa o indirectamente, afectan a esa esfera y aquellos otros en que no se incide en la autonomía de tales organismos, el obstáculo que supone la determinación de la competencia para clasificar los convenios en una u otra clase y la indeterminación en la propia LRJSP de los elementos que estructuran la autorización, que, no se olvide, es una técnica de control administrativo, justifican la improcedencia de exigir la autorización previa del Ministerio de Hacienda y Administraciones Públicas a los convenios que pretenda concertar el CSN, así como las demás entidades que ostenten la condición de autoridades administrativas independientes. En rigor, aunque el dictamen del Consejo de Estado no formulase

expresamente ningún reparo al artículo 25.2 del anteproyecto de Ley, no cabe duda de que las consideraciones expuestas por el Alto Cuerpo Consultivo a propósito del artículo 60 de dicho anteproyecto, y en las que se rechaza la sujeción de las entidades de continua referencia a controles que afecten a la neutralidad de éstas, son aplicables a la regla del artículo 50.2.b) de la LRJSP."

En otro orden de cosas, **sería igualmente preciso que se clarificase que los actos dictados por la Agencia española de Protección de Datos agotan la vía administrativa, siendo susceptibles de recurso contencioso-administrativo ante la Audiencia Nacional**.

En relación con su régimen presupuestario y de personal, debe recordarse nuevamente lo establecido en el artículo 52.4 del Reglamento general de Protección de Datos. De este modo, para que una norma interna resulte ajustada a dicho precepto deberá establecer las garantías necesarias para que la autoridad de control pueda ejercer sus funciones con total independencia y contar con los medios tanto materiales como personales suficientes para poder afrontar el desempeño de sus funciones y potestades.

El artículo 47 prevé que el presupuesto de la Agencia será elaborado y aprobado por la misma para su adecuada integración en los Presupuestos Generales del Estado, asimismo establece en su apartado 3 los elementos que configurarán su patrimonio, incluyendo los ingresos derivados del ejercicio de sus potestades, que se destinarán, en caso de ser el resultado positivo, a la dotación de sus reservas (apartado 4) y contará con personal funcionario o laboral, sometido a la legislación que le sea, respectivamente de aplicación (apartado 5).

El apartado 6 de este precepto prevé que la Agencia "contará con una relación de puestos de trabajo que deberá ser aprobada por el Ministerio de Hacienda y Función Pública en la que constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas".

Como se ha indicado, las Administraciones Públicas deberán dotar a la Agencia , por imperativo del Reglamento General de Protección de datos, de los medios necesarios para el cumplimiento de sus funciones, lo que exige, cuando menos, que sea la propia autoridad de protección de datos la que pueda delimitar cómo han de organizarse sus recursos. Ello impone que la Ley no debería limitarse a establecer que la relación de puestos de trabajo será aprobada por el Ministerio de Hacienda y Función Pública, sino al menos señalar que la capacidad de elaboración y propuesta de dicha relación de puestos de trabajo para su aprobación por el órgano competente corresponda a

la propia autoridad, partiendo del principio de total independencia que debe gobernar su funcionamiento.

Por este motivo, **se propone la siguiente redacción para el apartado 6 del artículo 47 del Anteproyecto**:

"La Agencia española de Protección de Datos **elaborará su** relación de puestos de trabajo, que **será** aprobada por el Ministerio de Hacienda y Función Pública **a propuesta de la misma. En dicha relación de puestos de trabajo** constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas."

Respecto de sus funciones y potestades, el artículo 48 se remite a las establecidas, respectivamente por los artículos 57 y 58 del Reglamento General de Protección de Datos, así como las contenidas "en la presente ley orgánica, en otras leyes, en sus disposiciones de desarrollo y en las demás normas de Derecho europeo".

A tal efecto, debe tenerse en cuenta que la Agencia Española de Protección de Datos no sólo ejerce las competencias derivadas del Reglamento, sino también ejercerá las que establece para las autoridades de protección de datos la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Igualmente ejerce actualmente las potestades derivadas de la Directiva 2002/58 el Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), que en la actualidad se recogen en la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

La enumeración de las fuentes normativas efectuada por el artículo 48 podría inducir a cierta confusión, dado que se entremezclan las normas directamente relacionadas con el Reglamento general de protección de datos y el Anteproyecto son otras establecidas en normas especiales. Por ello podría ser adecuado establecer una mejor sistemática del precepto diferenciando unas y otras.

En consecuencia, se propone la siguiente redacción del artículo 48:

"Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo Reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.

Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras Leyes u otras normas de derecho de la Unión Europea."

Por lo que respecta a su la estructura de la Agencia, resulta oportuna la modificación de la denominación de su órgano superior, que pasa a ser la de Presidente y no la de Director, lo que clarifica su rango, así como la ampliación del mandato de éste de cuatro a cinco años, que desvincula aquél del plazo de duración de las legislaturas y coincide en extensión con el establecido para el Supervisor Europeo de Protección de Datos en el artículo 42.1 del Reglamento 45/2001/CE del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Igualmente resulta oportuna la incorporación al Consejo Consultivo de un representante del Consejo General del Poder Judicial, dadas las competencias otorgadas al mismo por el artículo 236 nonies.1 de la Ley Orgánica del Poder Judicial.

Finalmente, en materia de trasparencia, y sin perjuicio de sus obligaciones de responsabilidad activa conforme a lo establecido en la Ley 19/2013, la Agencia hará públicas las resoluciones mencionadas en el artículo 51 así como las que se determinen en su estatuto, lo que implica el mantenimiento de la previsión contenida en el artículo 37.2 de la vigente Ley Orgánica 15/1999, según cuyo párrafo primero "Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos".

Ahora bien, hasta ahora la determinación del modo en que correspondía llevar a cabo la publicidad de las resoluciones de la Agencia Española de Protección de Datos correspondía en exclusiva a la propia Agencia, habiéndose dictado a tal efecto la Instrucción 1/2004, de 22 diciembre.

Sin embargo, el Anteproyecto indica que la forma en que se llevará a cabo la publicidad se establecerá "mediante real decreto"; es decir, será el Gobierno el que establezca el modo en que las resoluciones de la Agencia Española de Protección de Datos deban ser accesibles por terceros a fin de

conocer su contenidos y la propia interpretación que la Agencia realice de las normas de protección de datos.

A nuestro juicio, tal previsión choca con la independencia y la potestad de auto organización con que la Agencia debe estar dotada en esta materia, debiendo únicamente corresponder a la propia autoridad de protección de datos la competencia para determinar el modo en que se lleve a cabo esa publicidad.

Por ello, se propone la siguiente redacción del artículo 51 del Anteproyecto:

> "La Agencia Española de Protección de Datos publicará en la forma que **determine mediante Circular** las resoluciones de su Presidente que declaren haber lugar o no a la atención de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, las que pongan fin a los procedimientos de reclamación, las que archiven las actuaciones previas de investigación, las que sancionen con apercibimiento a las entidades a que se refiere el artículo 77.1 de esta ley, las que impongan medidas cautelares y las demás que disponga su Estatuto"

XXV

Las Secciones segunda y tercera del Capítulo I del Título VI del Anteproyecto regulan las potestades de la Agencia española de Protección de Datos, partiendo del régimen establecido en el artículo 58 del Reglamento General de Protección de Datos. A tal efecto, se regulan las potestades de investigación, regulación y acción exterior.

En cuanto a las potestades de investigación, podrán llevarse a cabo en el entorno de procedimientos concretos de reclamación, de los regulados por el Título VII del Anteproyecto o en el marco de los denominados planes de auditoría preventiva, regulados por el artículo 55 del Anteproyecto y que implican el reconocimiento legal expreso de los hasta ahora denominados "planes de inspección de oficio", en que sin la adopción de medidas coercitivas, la Agencia Española de Protección de Datos analiza el nivel de cumplimiento de las disposiciones aplicables en un determinado sector de actividad, adoptando las conclusiones que resultan pertinentes, así como recomendaciones, que conforme al artículo 55.3 recibirán la forma de directrices y "serán de obligado cumplimiento para el sector o responsable al que se refiera el plan de auditoría".

EL artículo 52 del Anteproyecto prevé que las actuaciones de inspección podrán levarse a cabo por el personal de la Agencia o "por funcionarios ajenos a ella habilitados expresamente por su Presidente".

Debe recordarse que esta posibilidad se encontraba prevista en el artículo 123.2 del reglamento de desarrollo de la Ley Orgánica 15/1999, según el cual “en supuestos excepcionales, el Director de la Agencia Española de Protección de datos podrá designar para la realización de actuaciones específicas a funcionarios de la propia Agencia no habilitados con carácter general para el ejercicio de funciones inspectoras o a funcionarios que no presten sus funciones en la Agencia, siempre que reúnan las condiciones de idoneidad y especialización necesarias para la realización de tales actuaciones. En estos casos, la autorización indicará expresamente la identificación del funcionario y las concretas actuaciones previas de inspección a realizar”. Dicho precepto fue anulado por la sentencia del Tribunal Supremo de 15 de julo de 2010 al no existir cobertura en la propia Ley Orgánica para establecer esta habilitación.

De este modo, la inclusión en el artículo 52.2 tiene por objeto dar fundamento legal a la habilitación que lleve a cabo el Presidente de la Agencia.

En todo caso, el precepto debe integrarse son la disposición adicional décimo tercera, a tenor de cuyo último inciso “la habilitación a la que se refiere el artículo 52.2 no podrán suponer incremento de dotaciones, ni de retribuciones, ni de otros gastos de personal”.

El artículo 53. 3 tiene por objeto determinar el régimen aplicable conforme a lo dispuesto en el artículo 62.3 del reglamento general de protección de datos, según el cual “una autoridad de control podrá, con arreglo al Derecho de su Estado miembro y con la autorización de la autoridad de control de origen, conferir poderes, incluidos poderes de investigación, a los miembros o al personal de la autoridad de control de origen que participen en operaciones conjuntas, o aceptar, en la medida en que lo permita el Derecho del Estado miembro de la autoridad de control de acogida, que los miembros o el personal de la autoridad de control de origen ejerzan sus poderes de investigación de conformidad con el Derecho del Estado miembro de la autoridad de control de origen. Dichos poderes de investigación solo podrán ejercerse bajo la orientación y en presencia de miembros o personal de la autoridad de control de acogida. Los miembros o el personal de la autoridad de control de origen estarán sujetos al Derecho del Estado miembro de la autoridad de control de acogida”.

En este sentido, el legislador español opta por la aplicación al personal de otras autoridades de control de las normas del propio Anteproyecto, sometiendo a dicho personal a la orientación del personal de la Agencia, bajo cuya presencia el personal de otras autoridades podrá desempeñar su actividad.

Los artículos 53 y 54 regulan el alcance de la actividad de investigación tanto en cuanto a la información que podrá ser recabada en el marco de las actuaciones concretas de inspección como en lo que respecta al deber de colaboración con el personal competente para la realización de estas actividades.

En particular, se hace referencia en el artículo 53 a la posible obtención de información de las Administraciones Públicas, y en particular de las tributarias y de seguridad social, con la finalidad de poder identificar al autor de una determinada conducta sancionable. Con ello se persigue únicamente evitar que entramados societarios puedan garantizar la impunidad de los autores de las conductas infractoras.

Igualmente, se prevé la posibilidad de que la Agencia española de Protección de Datos pueda acceder a datos de tráfico específicamente enumerados que permitan la identificación del autor de las conductas llevadas a cabo mediante la prestación de servicios de la sociedad de la información o el uso de comunicaciones electrónicas. En todo caso, quedan excluidos los datos que fueran exclusivamente conservados por los operadores de telecomunicaciones para el cumplimiento de las obligaciones contenidas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Se sigue así en este punto el criterio sentado por la Abogacía General del Estado en su Dictamen de 29 de diciembre de 2008, que considera lícito el acceso a los mencionados datos para el ejercicio de las competencias de inspección de la Agencia.

Por otra parte, el artículo 54 del Anteproyecto dispone en el último inciso del párrafo primero que “los poderes de investigación en lo que se refiere a entrada a domicilios y restantes lugares cuyo acceso requiera el consentimiento de su titular deben ejercerse de conformidad de acuerdo con las normas procesales, en particular, en los casos en los que sea precisa la autorización judicial previa”.

El artículo 8.6 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa atribuye a los juzgados de lo contencioso-administrativo la competencia para conocer “de las autorizaciones para la entrada en domicilios y restantes lugares cuyo acceso requiera el consentimiento de su titular, siempre que ello proceda para la ejecución forzosa de actos de la Administración pública”.

Quiere ello decir que de conformidad con lo dispuesto en la citada Ley así como en la jurisprudencia de nuestro tribunal Constitucional, efectivamente, la entrada en un domicilio particular para la realización de las actuaciones cuya competencia atribuye el Anteproyecto a la Agencia requerirá de la citada autorización judicial. No obstante, esta previsión ya aparece recogida en el

ordenamiento jurídico sin necesidad de que la misma sea objeto de reiteración por el artículo que ahora ha sido reproducido.

Por este motivo, y atendiendo a razones de técnica normativa, **se considera procedente la supresión del último inciso del párrafo primero del artículo 54 del Anteproyecto**.

El Anteproyecto regula igualmente a las potestades de regulación de la Agencia Española de Protección de Datos a través de Circulares. En este sentido, es preciso señalar que pese a no existir una norma similar en el articulado de la Ley Orgánica 15/1999, ya la sentencia del Tribunal Supremo de 16 de febrero de 2007, consideró que la Agencia ostentaba una potestad reglamentaria derivada, encaminada a ordenar la actuación de los operadores en lo que se refiere al tratamiento de los datos para su adecuación a los principios establecidos en la Ley. Dichas normas estaban dotadas de carácter obligatorio y eficacia "ad extra", y se materializaban en las denominadas Instrucciones de la Agencia. La Ley, por tanto, únicamente modifica la denominación de las disposiciones emanadas de la Agencia, asimilándola a la propia de otros organismos de supervisión.

Finalmente se regula la acción exterior de la Agencia, reiterando la condición de representante del Reino de España de la Agencia en el Comité Europeo de Protección de Datos. Además, se prevé la competencia de la Agencia cuando un Convenio internacional en que sea parte España prevea la existencia de autoridades de control en los Estados Parte, promoviéndose su participación en distintos órganos y foros internacionales así como su cooperación con otros Estados, con especial mención de los Iberoamericanos. Debe en este punto recordarse la creación en el año 2003 de la Red Iberoamericana de Protección de Datos, cuya contribución en el desarrollo de un marco normativo en distintos estados de la región ha sido comúnmente reconocida.

XXVI

El Capítulo II del Título VI del Anteproyecto, bajo la rúbrica “autoridades autonómicas de protección de datos”, regula el papel de estas autoridades y los procedimientos de cooperación entre las mismas y la Agencia Española de Protección de Datos.

La Ley Orgánica 5/1992, de 24 de octubre, reguladora del Tratamiento automatizado de datos de carácter personal, creó la Agencia Española de Protección de Datos, previendo igualmente la posibilidad de que las Comunidades Autónomas creasen, en su caso, autoridades de control, cuyas competencias se circunscribirían a los ficheros de los que fueran responsables las administraciones de las propias Comunidades.

Posteriormente, la Ley 15/1999 amplió las competencias de las autoridades autonómicas a las entidades locales situadas en el territorio de las Comunidades Autónomas.

Finalmente, diversos Estatutos de Autonomía han previsto en su articulado la posible creación de una autoridad de protección de datos encargada de velar por los tratamientos anteriormente mencionados y los previstos en sus Estatutos de Autonomía.

Este modelo se completa con la doctrina emanada del Tribunal Constitucional en su sentencia 290/2000, de 30 de diciembre, que viene a declarar expresamente que la competencia en lo referente al tratamiento de datos de carácter personal por parte de las entidades de derecho privado habrá de ser de exclusiva competencia de la Agencia Española de Protección de Datos, a fin de garantizar una protección uniforme del derecho fundamental en todo el territorio español.

La Ley Orgánica mantiene el esquema que se venía recogiendo en sus antecedentes normativos. De este modo, las competencias propias de las autoridades de control corresponderán a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las Comunidades Autónomas, si bien la competencia de éstas se refiere a la que ya aparecía prevista en el artículo 41 de la Ley Orgánica 15/1999, completada en su caso por lo previsto en el correspondiente Estatuto de Autonomía.

El Anteproyecto prevé en su artículo 59 el establecimiento de mecanismos de cooperación mediante el mantenimiento de encuentros periódicos y el intercambio de información necesaria para el adecuado cumplimiento por todas las autoridades, en su ámbito competencial, de lo establecido en el Reglamento General de Protección de Datos.

Por su parte, el artículo 60 mantiene el mecanismo establecido en el artículo 42 de la Ley Orgánica 15/1999 para los supuestos de incumplimiento por las Administraciones Autonómicas en las que exista una autoridad autonómica de protección de datos de las disposiciones de la Ley Orgánica 15/1999. No obstante, el precepto se clarifica en cuanto a su redacción y toma particularmente en consideración el papel de las citadas autoridades autonómicas, por cuanto la Agencia Española pondrá la situación previamente en su conocimiento, a fin de que sea ésta la que adopte las medidas oportunas, que la Agencia Española únicamente adoptará en caso de que la autoridad autonómica no adoptase las medidas oportunas en el plazo de un mes. Si la Administración autonómica desatendiera los requerimientos de la Agencia Española de Protección de Datos, ésta podrá impugnar la actividad o inactividad de dicha Administración ante la jurisdicción contencioso-

administrativa, gozando así de legitimación activa para la interposición del correspondiente recurso.

El Anteproyecto regula igualmente el mecanismo de coordinación entre la Agencia Española de Protección de datos y las autoridades autonómicas de protección de datos en los supuestos en que éstas últimas, o ambas, pudieran verse afectadas por el procedimiento de cooperación establecido en el Reglamento General de Protección de Datos o en los casos en que las autoridades autonómicas hubieran de solicitar el Comité Europeo de Protección de Datos la emisión de dictamen en los asuntos previstos en los apartados 1 y 2 del artículo 64 de dicho texto legal, teniendo en cuenta que la Agencia Española de Protección de Datos tiene la condición de representante único de España ante el Comité.

Ciertamente no serán abundantes los casos en los que sea aplicable el primero de los supuestos enunciados, habida cuenta del ámbito competencial de las autoridades autonómicas, lo que sin embargo no puede ser óbice para garantizar la coordinación en este punto. Se parte del principio de que la condición de autoridad principal sólo concurrirá en las autoridades autonómicas en los supuestos en los que la actuación se dirija a responsables que no lleven a cabo el mismo tipo de tratamiento al que se refiera el asunto en el resto del territorio español; en este caso, sería la Agencia española la que ostentaría la condición de autoridad principal, teniendo en cuenta la doctrina sentada por el Tribunal Constitucional en su sentencia 290/2000, de 30 de noviembre.

En todo caso, los mecanismos establecidos pasan por el respeto a la posición de las autoridades autonómicas de protección de datos cuando a ellas corresponda la iniciativa. Así, la Agencia Española de Protección de Datos será asistida por un representante de la propia autoridad autonómica interesada.

XXVII

El Título VII del Anteproyecto regula los procedimientos en caso de reclamaciones tramitadas por la Agencia Española de Protección de Datos

En este punto, es preciso señalar que el Reglamento general de protección de datos establece un régimen sumamente complejo en lo que se refiere a la tramitación de los procedimientos en caso de presentación de una reclamación contra un responsable o encargado del tratamiento.

Para poder diferenciar claramente estos supuestos deben tenerse en cuenta dos criterios previos de delimitación: la naturaleza del tratamiento al que se refiera la reclamación y el papel de la autoridad nacional interviniente en el mismo.

En cuanto a la naturaleza del tratamiento, deberán diferenciarse tres posibles supuestos diferenciados en atención a la afección del tratamiento a uno o varios Estados miembros.

Así, en primer lugar, se puede hacer referencia a los tratamientos transfronterizos, que son definidos por el artículo 4.23 del Reglamento general de protección de datos, que los divide en dos posibles categorías:

> "a) El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro.
>
> b) El tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro."

Junto con estos tratamientos puede hacerse referencia a una segunda categoría, conformada por los denominados tratamientos transfronterizos con relevancia local, cuyo régimen derivaría de los apartados 2 a 4 del artículo 56 del Reglamento. Se trataría de los tratamientos realizados por un establecimiento de un responsable en la Unión (que tiene varios establecimientos en ella) y que, en principio sólo afectan de manera sustancial a ciudadanos del Estado de ese establecimiento

Por último cabría hacer referencia a los tratamientos puramente nacionales, llevados a cabo por un responsable con establecimiento en un Estado y dirigidos a ciudadanos de ese Estado. Incluyen los realizados por el sector público y los que se lleven a cabo en cumplimiento de una obligación legal, tal y como establece el artículo 55.2 del Reglamento.

El segundo elemento a tener en cuenta en el régimen procedimental del Reglamento es el papel de la autoridad nacional que intervenga en el procedimiento, para lo que habrá que determinar cuál es la denominada autoridad principal, que correrá con el peso del procedimiento y diferenciarla de las restantes autoridades, que tendrán la condición de interesadas. A tal efecto, es relevante tener en cuenta que una autoridad puede tener la condición de interesada incluso aunque no se haya formulado ante ella ninguna reclamación ni sea la autoridad del establecimiento principal del responsable o encargado contra el que se dirija el procedimiento.

Hecha esta primera consideración, y en lo que atañe propiamente al procedimiento, el Reglamento general de protección de datos impone, cuando

haya varias autoridades implicadas, la necesidad de que todas ellas lleguen a un acuerdo o, a falta de este, que el acuerdo se adopte por el Comité Europeo de Protección de Datos, estableciéndose peculiaridades en cada caso. Este procedimiento será distinto en caso de que nos encontremos ante un tratamiento transfronterizo o ante un tratamiento transfronterizo con relevancia local.

Si el tratamiento es transfronterizo, el íter del procedimiento podría desglosarse en las siguientes fases:

- En primer lugar, sería preciso determinar qué autoridad de control tiene la condición de autoridad de control principal, para lo que habrá de tenerse en cuenta el concepto de establecimiento principal establecido en el artículo 4.16 del Reglamento general de protección de datos. En caso de que las autoridades interesadas no llegasen a un acuerdo sobre la determinación de la autoridad principal la decisión correspondería al Comité Europeo de Protección de Datos, conforme al artículo65.1 b) del Reglamento.

- A partir de esta determinación, la autoridad principal proseguirá con la tramitación del procedimiento conforme a su derecho nacional. Durante esta tramitación, que podrá incluir actuaciones inspectoras, se prevé expresamente la posibilidad de que se realicen actuaciones conjuntas de investigación (artículo 62), debiendo en todo caso las autoridades prestarse la asistencia mutua que requieran (artículo 61).

- Concluida la tramitación, la autoridad de control principal adoptará un “proyecto de decisión”, que comunicará sin dilación a las restantes autoridades interesadas para obtener su opinión al respecto en el plazo de tres semanas (artículo 60.3 del reglamento general de Protección de datos).

- Las autoridades interesadas podrán emitir en ese plazo, conforme al artículo 60.4, una “objeción pertinente motivada”, definida por el artículo 4.24 del reglamento general de protección de datos como “la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión”.

- Formuladas en su caso las citadas objeciones, la autoridad de control principal podrá optar por no seguirlas, en cuyo caso someterá la cuestión al Comité Europeo de Protección de Datos, conforme al artículo

63, o adoptar un “proyecto de decisión revisado”, respecto del que se volverá a dar traslado a las restantes autoridades interesadas para conocer su parecer en el plazo de dos semanas

- En caso de nueva discrepancia la cuestión se someterá a la decisión del Comité Europeo de Protección de Datos, que tendrá carácter vinculante.

Además, el Reglamento establece un régimen especial en cuanto a qué autoridad deberá dictar la resolución. Así, el artículo 60.9 establece que “En caso de que la autoridad de control principal y las autoridades de control interesadas acuerden desestimar o rechazar determinadas partes de una reclamación y atender otras partes de ella, se adoptará una decisión separada para cada una de esas partes del asunto. La autoridad de control principal adoptará la decisión respecto de la parte referida a acciones en relación con el responsable del tratamiento, la notificará al establecimiento principal o al único establecimiento del responsable o del encargado en el territorio de su Estado miembro, e informará de ello al reclamante, mientras que la autoridad de control del reclamante adoptará la decisión respecto de la parte relativa a la desestimación o rechazo de dicha reclamación, la notificará a dicho reclamante e informará de ello al responsable o al encargado”.

De este modo, es perfectamente posible que la tramitación del procedimiento se lleve a cabo por una autoridad distinta de la que deba dictar la resolución que ponga término al mismo, siendo incluso posible que existan dos resoluciones dictadas por distintas autoridades que pongan término a un único procedimiento.

Si el procedimiento es transfronterizo con relevancia local, la autoridad ante la que se presente la reclamación (y en cuyo Estado existe un establecimiento del responsable) deberá plantearle a la autoridad del establecimiento principal si desea tramitar el procedimiento, debiendo ésta pronunciarse sobre la cuestión en tres semanas.

- Si considera procedente tramitar el procedimiento, se estará a las reglas del procedimiento transfronterizo, debiendo tenerse particularmente en cuenta la opinión de la autoridad ante la que se presentó la reclamación.
-
- Si no considera procedente tramitarlo, el procedimiento se seguirá por la autoridad ante la que se formuló la reclamación como si el tratamiento no tuviese un carácter transfronterizo.

En consecuencia, con anterioridad a la tramitación de cualquier procedimiento será preciso determinar el tipo de tratamiento ante el que nos encontramos y qué autoridad ostenta la condición de principal, sin poder iniciar la tramitación hasta entonces. Ello se debe a que si bien en muchos casos estas cuestiones serán fáciles de dirimir no siempre será posible conocer a

simple vista la naturaleza multinacional del responsable o encargado o el Estado en que se encuentra su establecimiento principal.

Al propio tiempo, dada la naturaleza necesariamente coordinada de los procedimientos transfronterizos será necesario establecer normas sobre la lengua en que se desarrollarán, al menos los trámites que lleve a cabo otra autoridad o los proyectos o proyectos de decisión y las objeciones pertinentes y motivadas de las distintas autoridades.

De todo lo que se viene indicando cabe concluir que el régimen previsto en el Reglamento general de protección de datos contempla hasta siete posibles procedimientos diferenciados en que pudiera intervenir la Agencia Española de Protección de Datos:

- Procedimiento en caso de tratamientos puramente nacionales, tramitados con arreglo a las normas generales del procedimiento que se establezcan. Este mismo procedimiento será aplicable a los supuestos de tratamiento transfronterizo con relevancia local en España respecto a responsables que tengan en España su establecimiento principal (por ejemplo, reclamaciones en España relacionadas con tratamientos llevados a cabo por una entidad financiera de nacionalidad española).

- Procedimiento en caso de tratamientos transfronterizos con relevancia local en España cuando la autoridad principal fuese la de otro Estado Miembro (por ejemplo, reclamaciones en España contra tratamientos llevado a cabo en España por un operador de telecomunicaciones cuya matriz se encuentre en otro Estado Miembros) y dicha autoridad (la del Estado Miembro de la matriz) decida tramitar el procedimiento.

- Procedimiento en caso de tratamientos transfronterizos con relevancia local en otro Estado miembro en que el establecimiento principal esté en España (por ejemplo, reclamaciones contra la filial en otro Estado Miembros de un operador de telecomunicaciones español) y la autoridad española decida tramitar el procedimiento.

- Procedimiento en caso de tratamientos transfronterizos “puros” en que se formulase reclamación (entre otras o junto con otras) ante la autoridad española y ésta fuera la del establecimiento principal (por ejemplo, reclamaciones contra la tienda on-line de una empresa española, incluyendo alguna de ellas en España).

- Procedimiento en caso de tratamientos transfronterizos “puros” en que no se formulase ninguna reclamación ante la autoridad española pero ésta fuera la autoridad del establecimiento principal (por ejemplo, quejas en varios países contra la tienda on-line de la empresa española, sin que existan reclamaciones ante la Agencia Española).

- Procedimiento en caso de tratamientos transfronterizos “puros” en que se formulase una reclamación ante la autoridad española y ésta no tuviese la condición de autoridad del establecimiento principal (por ejemplo, reclamaciones en España contra una red social cuyo establecimiento principal se encuentre en otro estado miembro).

- Procedimiento en caso de que se tenga conocimiento de la existencia de una reclamación relacionada con un tratamiento transfronterizo “puro” llevado a cabo por una entidad respecto de la que la autoridad española no ostenta la condición de autoridad principal y no existen reclamaciones en España, pero el tratamiento puede afectar a quienes se encuentre en España (por ejemplo, reclamaciones en varios Estados miembros contra los servicios on-line de una línea aérea que opera en España).

Cada procedimiento deberá tener unas especialidades propias, aunque existirán trámites parcialmente similares en varios de ellos. Debe optarse por el establecimiento de un procedimiento general para el primero de los casos citados y especialidades para los restantes, teniendo en cuenta que cuando la autoridad principal sea española podrán aplicarse hasta el proyecto de decisión las disposiciones generales. Igualmente deberá tenerse en cuenta la posibilidad de que existan procedimientos que no se tramiten por la autoridad española pero respecto de los que ésta tenga que dictar resolución, tal y como se ha indicado con anterioridad.

La descripción que se ha llevado a cabo lo es con el objeto de poner de manifiesto la imposibilidad material de que las normas contenidas en la Ley 39/2015, de 1 de octubre, de Procedimiento administrativo del sector público, sean aplicables, ni siquiera supletoriamente, a los procedimientos que la Agencia Española de Protección de Datos habrá de tramitar con arreglo al régimen establecido en el Reglamento.

Por este motivo, el artículo 64.1 del Anteproyecto establece que “Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos”.

En este sentido, el Anteproyecto opta por la aplicación del principio de subsidiariedad, que no de supletoriedad, de las normas generales de procedimiento administrativo, entendida en el sentido mencionado en la sentencia de la Audiencia Nacional de 23 de octubre de 2001, cuando recordaba que “el recurso a la subsidiariedad es una fórmula de colaboración normativa para los casos de concurso de normas, esto es, para los casos en los que resulten aplicables dos o más de ellas al mismo supuesto de hecho, de

manera que la subsidiaria cede en beneficio de la primaria a la que, en su caso, complementa", a diferencia de la supletoriedad, que tiene por objeto colmar una laguna "de tal manera que cuando un determinado supuesto no es objeto de regulación por la norma inicialmente aplicable se da paso a la supletoria, siempre, eso sí, que semejante operación no resulte, por otras circunstancias, disconforme al ordenamiento jurídico".

XXVIII

Partiendo del principio de aplicación únicamente subsidiaria y no supletoria de las normas generales del procedimiento administrativo, el Anteproyecto dedica el Título VII a establecer determinadas especialidades del procedimiento tramitado por la Agencia Española de Protección de Datos, dejando a un futuro desarrollo reglamentario la regulación de "los procedimientos aplicables a las reclamaciones formuladas por las personas físicas y las demás actuaciones cuya tramitación corresponda a la Agencia Española de Protección de Datos (…), asegurando en todo caso los derechos de defensa y audiencia de los interesados".

En este sentido, debe ponerse de manifiesto que las normas procedimentales que se han descrito en el apartado anterior del presente informe serán plenamente aplicables el día 25 de mayo de 2017 tal y como establece el artículo 99.2 del Reglamento General de Protección de Datos. Por ello, **se pone de relieve la necesidad de que a la mayor brevedad se adopte la norma reguladora de la integridad de dichos procedimientos**, a fin de garantizar que la misma entre en vigor al mismo tiempo que lo haga el Anteproyecto ahora sometido a informe.

Entrando ya en las disposiciones incluidas en el Anteproyecto, el artículo 65.1 prevé que los procedimientos se iniciarán de oficio o en virtud de reclamación, indicándose acto seguido que "Con carácter previo a su iniciación, la Agencia Española de Protección de Datos examinará su competencia y determinará el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir o remitirá la reclamación formulada a la Autoridad de control principal que considere competente".

Ello plantea una evidente contradicción, toda vez que si el acto iniciador del procedimiento es la presentación de una reclamación por parte de un interesado, la Agencia no podrá, con carácter previo a dicho acto, llevar a cabo las actuaciones a las que se refiere el apartado 2 del artículo 65.

Si se atiende al procedimiento actualmente vigente, cabe diferenciar en esta materia dos procedimientos distintos: el de tutela de derechos, que se iniciaría mediante la solicitud del interesado, y el sancionador o de declaración de infracción de las Administraciones Públicas, que siempre se iniciaría de

oficio. La extrapolación de esta distinción al régimen previsto en el Reglamento general de Protección de Datos es, no obstante, compleja, dado que incluso en los supuestos de tutela de derechos, será posible la tramitación del procedimiento al que se ha hecho referencia en el apartado anterior de este informe.

De este modo, sólo sería posible interpretar en sus propios términos el apartado 2 del artículo 65 del Anteproyecto en caso de que el procedimiento se iniciase siempre de oficio, dado que en otro caso resulta en todo punto imposible que la Agencia pueda llevar a cabo el análisis mencionado "con carácter previo" a la iniciación del procedimiento.

En caso de no considerarse adecuada la opción que acaba de indicarse, sería preciso modificar ambos apartados, de forma que se clarifique en el primer de ellos que la iniciación sólo tendrá lugar por reclamación si la misma se refiere exclusivamente a la falta de atención de los derechos recogidos en los artículo 25 a 22 del Reglamento general de protección de datos, indicando asimismo en el apartado 2 que las actuaciones que en él se describen tendrán lugar con carácter previo al inicio del procedimiento si este se produjese de inicio o inmediatamente después de presentada la reclamación cuando ésta supusiera la iniciación del procedimiento.

Como última solución posible, cabría considerar que la iniciación del procedimiento tendrá lugar como consecuencia de la admisión a trámite de la reclamación formulada, lo que permitiría, por una parte, realizar el examen al que se refiere el apartado 2 con carácter previo a la iniciación del procedimiento y, por otra parte, inadmitir a limine, conforme se analizará inmediatamente las reclamaciones que no versen sobre la materia, no aporten evidencias o resulten infundadas o abusivas.

Por otra parte, el artículo 66 establece los supuestos en que procederá inadmitir *a limine* las reclamaciones presentadas ante la Agencia, indicando que "La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos de carácter personal, carezcan manifiestamente de fundamento, sean abusivas o no se aporten elementos que permitan investigar la existencia de una vulneración de los derechos reconocidos".

Si bien el contenido de los supuestos mencionados en el artículo resulta el adecuado, cabría plantearse si este precepto no debería también preceder a lo dispuesto en el artículo 65.2, dado que la inadmisión será previa a cualquier actuación llevada a cabo por la Agencia para comprobar su competencia, determinar la naturaleza del tratamiento o reenviar el expediente a la autoridad que se considere competente.

Por ello, se considera que este precepto debería aparecer como apartado 2 del artículo 65.

A su vez, el apartado 3 del artículo 65 se refiere a los supuestos en que no continuará la tramitación del procedimiento al considerarse suficiente que por la Agencia española de Protección de Datos se remita una advertencia al presunto infractor en caso de que se aprecien determinados requisitos que el precepto cita.

La advertencia aparece expresamente recogida entre las medidas que podrán imponer las autoridades de control en caso de incumplimiento de las disposiciones del Reglamento conforme al artículo 83.2, por remisión al artículo 58 del mismo. No obstante, tal y como se indica, la adopción de esta medida implica la no iniciación del procedimiento, por lo que se volvería a producir una contradicción con lo dispuesto en el apartado 1, dado que la reclamación habría dado lugar a la iniciación del procedimiento

De todo lo que se ha venido indicando se desprende que la única posibilidad de hacer compatible la totalidad de las medidas a las que se ha hecho referencia será la de establecer una primera fase de admisión a trámite de la reclamación que se hubiese formulado por un interesado. Todo ello conduce necesariamente a una revisión de lo dispuesto en los artículos 65 y 66 del Anteproyecto, para lo que se propone la adopción de un único precepto que englobe a ambos bajo la siguiente redacción:

"Artículo 65. Iniciación de los procedimientos **y admisión a trámite**

1. Los procedimientos **regulados en este Capítulo se iniciarán cuando se acuerde por la Agencia Española de Protección de Datos la admisión a trámite de la reclamación formulada ante la misma**.

2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos de carácter personal, carezcan manifiestamente de fundamento, sean abusivas o no se aporten elementos que permitan investigar la existencia de una vulneración de los derechos reconocidos.

3. Cuando las reclamaciones no se hayan formulado previamente ante el delegado de protección de datos designado por el encargado o responsable del tratamiento o ante el organismo de supervisión establecido para la aplicación de los códigos de conducta, la Agencia podrá remitírselas**, antes de resolver la admisión a trámite,** a los efectos previstos en los artículos 38 y 39.3.

4. **Igualmente, antes de la admisión a trámite de la reclamación, la Agencia Española de Protección de Datos podrá resolver no iniciar**

el procedimiento cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio al afectado en el caso de las infracciones previstas en el artículo 74.

b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

5. Con carácter previo **a la admisión a trámite de la reclamación**, la Agencia Española de Protección de Datos examinará su competencia y determinará el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir o remitirá la reclamación formulada a la Autoridad de control principal que considere competente.

6. La decisión sobre la admisión o inadmisión a trámite, así como la que determine en su caso la remisión de la reclamación a la autoridad de control principal que se estime competente deberá notificarse al reclamante en el plazo de tres meses.

Si no se produjera dicha notificación, se entenderá que el procedimiento se ha iniciado en la fecha en que se cumpliesen tres meses desde que tuvo entrada en la Agencia española de Protección de Datos la reclamación."

Como consecuencia de esta propuesta, debería igualmente modificarse el apartad 1 del artículo 67, indicando que:

"Los plazos máximos de tramitación de los procedimientos y notificación de las resoluciones que los terminen se establecerán mediante real decreto, que no podrá fijar un plazo superior a 18 meses **a contar desde la fecha de admisión a trámite de la reclamación**."

Por último, el artículo 69 regula las medidas cautelares, señalándose en su apartado 3 que "La imposición de la obligación anticipada de atender el derecho solicitado por el afectado en su reclamación requerirá la previa audiencia del responsable del tratamiento".

Este supuesto parece referirse a aquellos casos en que el reclamante solicite de la Agencia Española de Protección de Datos tanto la atención de uno de los derechos establecidos por los artículos 15 a 22 del reglamento general de protección de datos como la adopción de medidas coercitivas contra el responsable. En estos casos, si la Agencia apreciase que procede atender el

derecho del afectado el procedimiento adecuado para garantizar su indemnidad será la adopción de dicha medida sin perjuicio de la tramitación del procedimiento sancionador, sin que el afectado haya de esperar a la adopción dela resolución final de este procedimiento para ver atendido su derecho.

Sin embargo, los términos del precepto no resultan a juicio de esta Agencia suficientemente claros, por lo que sería precisa su modificación a fin de clarificar el supuesto al que se está haciendo referencia con este precepto. Por este motivo, se propone la siguiente redacción del apartado 3 del artículo 69:

> "**Cuando la reclamación presentada ante la Agencia se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá acordar con anterioridad a la apertura del procedimiento, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado., prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.**"

XXIX

El Título VIII del Anteproyecto contiene finalmente las normas reguladoras del régimen sancionador

En esta materia, el Reglamento General de Protección de Datos establece un sistema de sanciones o actuaciones correctivas sumamente genérico, en que no se tipifican las conductas ni se establecen las reacciones concretas ante su comisión, más allá de la enumeración en los apartados 4 a 6 del artículo 83 de las sanciones que podrán imponerse, con un espectro amplísimo que puede llegar a alcanzar los 20 millones de euros o, en caso de ser superior, el 4 por 100 del volumen de negocio total anual global en el ejercicio financiero anterior a su imposición. De este modo, los citados apartados, que resultan los más aproximados a lo que podría considerarse desde el punto de vista de nuestro derecho interno, un régimen sancionador, establece que:

> "4.Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía”

Si bien el Reglamento General de Protección de Datos no habilita a los Estados miembros para establecer un catálogo de infracciones, sí es posible que el Anteproyecto pueda describir, de la forma más detallada posible las conductas típicas. De este modo, el texto sometido a informe describe en sus artículos72 a 74 dichas conductas, manteniendo la distinción entre infracciones

muy graves, graves y leves, a la vista de la diferenciación que el Reglamento General de Protección de Datos establece al fijar la cuantía de las sanciones.

Así, se consideran muy graves las conductas que pueden encuadrarse en los artículos 83.5 y 83.6 del Reglamento, considerándose graves las que se corresponden con el artículo 83.4. Finalmente, se consideran leves las infracciones de carácter meramente formal que pudieran incardinarse en dichos artículos del Reglamento. Es importante señalar que la graduación mencionada no es similar a la establecida en otras normas de derecho español, dado que con la categorización del Reglamento las sanciones no pueden "ser", sino "considerarse" leves, graves o muy graves.

La categorización de las infracciones que se acaba de mencionar afecta también a sus plazos de prescripción. El Reglamento General de Protección de Datos sujeta esta cuestión a la legislación de los Estados miembros, al no establecer norma alguna al respecto. Así, el Anteproyecto opta por mantener los plazos de tres años para las infracciones consideradas muy graves, dos para las consideradas graves y uno para las consideradas leves, tal y como se establece con carácter general en el artículo 30.1 de la Ley 40/2015, de 1 de octubre.

Se regulan además por el Anteproyecto los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento por parte de aquél contra el que se dirija el procedimiento de los hechos que se le imputan, pero teniendo igualmente en cuenta la problemática derivada de los procedimientos establecidos en el Reglamento General de Protección de Datos. Así, cabrá diferenciar los supuestos en que haya de acudirse al procedimiento establecido en el artículo 60 del Reglamento General de Protección de Datos y aquéllos en que no sea preciso tener en cuenta lo previsto en aquél, dada la naturaleza exclusivamente local del tratamiento.

Si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos, la Ley mantiene el criterio general consagrado en la Ley 39/2015, de 1 de octubre, reguladora del Procedimiento administrativo común de las Administraciones Públicas, que prevé la interrupción de la prescripción cuando el interesado tenga conocimiento de la apertura del procedimiento. Si, por el contrario, fuese necesario acudir al procedimiento coordinado establecido en el artículo 60 del Reglamento y la Agencia Española de Protección de Datos tuviese la condición de autoridad de control principal, se prevé que dicha interrupción tendrá lugar cuando el interesado conozca el proyecto de acuerdo de inicio que hubiera haber adoptado la Agencia Española de Protección de Datos para su comunicación a las restantes autoridades de control interesadas.

En cuanto a las sanciones, el Reglamento General de Protección de Datos establece los criterios para la determinación de su cuantía, dentro de los

amplios márgenes que prevé. Dentro de dichos criterios el apartado 2 del artículo 83 del reglamento incorpora una cláusula residual, referida a los restantes factores agravantes o atenuantes aplicables al caso. A la vista de esta cláusula, la Ley Orgánica aclara que entre los elementos a tener en cuenta en la aplicación de esa cláusula podrán incluirse los que ya aparecen recogidos en los apartados 4 y 5 del artículo 45 de la Ley Orgánica 15/1999, y que son conocidos por los operadores jurídicos en este ámbito de actividad. De este modo, se indica la posibilidad de tener en cuenta los criterios procedentes de esos preceptos, que no se encuentran expresamente recogidos en el artículo 83 del Reglamento General de Protección de Datos.

Por otra parte, el artículo 77 hace uso de la previsión establecida en el artículo 83.7 del Reglamento General de Protección de Datos, manteniendo el principio de la no imposición de sanciones económicas a las entidades y organismos que configuran lo que podría denominarse sector público. Cuando la infracción fuese cometida por los responsables enumerados taxativamente en ese precepto, procederá imponer la sanción de apercibimiento. Se configura así el apercibimiento como una sanción, siguiendo lo previsto en el Reglamento General de Protección de Datos, frente a la naturaleza no sancionadora que le atribuye actualmente la Ley Orgánica 15/1999. A fin de garantizar el principio de transparencia en el funcionamiento de las Administraciones Públicas, la Ley prevé que las resoluciones impuestas a estas categorías de responsables del tratamiento serán en todo caso objeto de una publicación clara y separada en la página web de la Agencia Española de Protección de Datos.

En cuanto a la prescripción de las sanciones, la Ley Orgánica ha considerado oportuno el mantenimiento de los términos establecidos en la Ley Orgánica 15/1999. De este modo, aun cuando las cuantías de las sanciones pudieran sufrir un notable incremento a la vista de las previsiones del Reglamento General de Protección de Datos, esta circunstancia no afectaría a los plazos máximos de prescripción, que se mantienen de forma coherente con los previstos en la Ley 39/2015.

XXX

Deben por último analizarse las disposiciones adicionales, transitorias y finales contenidas en el Anteproyecto y que no han sido mencionadas con anterioridad.

Así, la disposición adicional tercera regula el cómputo de plazos que será de aplicación a la Ley. Es preciso indicar que dicha previsión resulta necesaria, por cuanto no sólo se trata de establecer el modo en que se computarán los trámites de los procedimientos tramitados por las autoridades de protección de datos, sino que la disposición extiende su eficacia sobre la totalidad de los términos y plazos establecidos a lo largo de la misma. Con la

fijación de una regla concreta de cómputo de los plazos se trata de uniformizar el cómputo para los sujetos de derecho público y de derecho privado, de modo que para todos ellos sólo existirán unas normas de cómputo. Así, por ejemplo, en los plazos establecidos por días para sujetos de derecho privado se excluirán los sábados, en aplicación del apartado a) de la disposición, siendo así que esta exclusión sólo operaría para los sujetos de derecho público si no se hubiera incorporado la disposición adicional a la que se está haciendo referencia.

Resulta igualmente relevante lo establecido por la disposición adicional undécima, que establece reglas para la minimización de los datos contenidos en notificaciones por medio de anuncios, al señalar que “cuando la notificación por medio de anuncios o la publicación de un acto administrativo contuviese datos de carácter personal del destinatario, se identificará al mismo mediante las iniciales de su nombre y de sus dos apellidos y su número de documento nacional de identidad”.

En este sentido, debe recordarse que las Administraciones Públicas incorporan a esas notificaciones y publicaciones datos de los destinatarios que en un gran número de supuestos no resultan necesarios para garantizar la efectividad de la publicación o notificación, vinculado casi siempre el nombre y apellidos de la persona al número de su documento nacional de identidad. Ello, unido a la publicación en tablones edictales electrónicos hace que en un gran número de supuestos resulte sumamente sencilla la vinculación del nombre y apellidos de la persona con su documento, lo que podría facilitar a su vez su suplantación en un gran número de servicios de contratación a distancia.

En este punto, debe recordarse que, conforme al artículo 1.2 del Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, dispone que el citado documento “tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo”. Es decir, el destinatario de la notificación queda suficientemente identificado mediante la mera inclusión de su documento nacional de identidad, sin necesidad de añadir al mismo su nombre y apellidos. Por ello, se prevé que sólo se incorpore, en adición al número del documento, las iniciales de los interesados, siendo la información suficiente para que la notificación produzca todos sus efectos y minimizando el riesgo derivado del sistema actual.

La disposición adicional duodécima establece que “Cuando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos”. Esta previsión se encontraba recogida en el artículo 11 del Reglamento de

desarrollo de la Ley Orgánica de Protección de Datos, habiendo sido anulada por la sentencia del Tribunal Supremo de 15 de julio de 2010, al considerarse que carecía de cobertura legal suficiente, lo que se lleva a cabo a través de esta disposición adicional, al poder considerarse que el tratamiento se llevaría a cabo en el ejercicio de poderes públicos, conforme al artículo 6.1 e) del reglamento general de Protección de Datos.

Respecto de las disposiciones transitorias, merecen especial referencia la cuarta y la quinta.

La primera de ellas prevé que permanecerán vigentes, en cuanto no se proceda a su modificación o derogación, las normas en que se hubiera establecido, al amparo del artículo 13 de la Directiva 95/46/CE, alguna excepción al cumplimiento del deber de información o al ejercicio de los derechos de acceso, rectificación, cancelación u oposición y que se encontrasen en vigor, y particularmente lo dispuesto en los artículos 23 y 24 de la Ley Orgánica 15/1999. Estas normas deberán ser, en su caso, revisadas en el futuro, a fin de incorporar las exigencias las que se refiere el apartado 2 del artículo 21 del Reglamento General de Protección de Datos.

La disposición transitoria quinta declara que, a pesar de lo que prevé la disposición derogatoria, la Ley Orgánica 15/1999 y sus disposiciones de desarrollo serán de aplicación a los tratamientos que se llevasen a cabo en el marco de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales en tanto no entre en vigor la norma que trasponga al ordenamiento español la Directiva (UE) 2016/680, reguladora de esos tratamientos.

Como es sabido, el artículo 2.2 b) del Anteproyecto excluye los citados tratamientos de su ámbito de aplicación, al no serles de aplicación el reglamento general, sino la citada Directiva. Sin embargo, resulta necesario establecer una cautela sobre su legislación aplicable en tanto no se produzca la trasposición al derecho español de la citada Directiva. Para ello se ha considerado como mejor solución posible por el Anteproyecto que las normas contenidas en la Ley Orgánica 15/1999, que son actualmente de aplicación a dichos tratamientos lo sigan siendo en tanto no se proceda a la definitiva derogación de la norma como consecuencia de la trasposición de la Directiva (UE) 2016/680.

Como consecuencia de estas disposiciones, la disposición derogatoria de la Ley Orgánica 15/1999 lo es, lógicamente, sin perjuicio de lo previsto en las mismas.

Por último, cabe hacer referencia a la disposición final tercera, por la que se modifica el artículo 15 bis de la Ley de Enjuiciamiento Civil a efectos de otorgar a la Agencia Española de Protección de Datos la condición de *amicus*

curiae en los procedimientos civiles que afecten al derecho fundamental a la protección de datos, en términos similares a los previstos actualmente para la Comisión Nacional de los Mercados y la Competencia

En este punto, el artículo 58.5 del Reglamento General de Protección de Datos establece que "cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo".

Ello exige que se introduzcan en el derecho interno normas que reconozcan la legitimación procesal activa de las autoridades de protección de datos para entablar acciones en defensa del derecho fundamental a la protección de datos de carácter personal cuando el mismo haya sido vulnerado, permitiendo asimismo que dichas autoridades de protección de datos puedan intervenir como *amicus curiae*, de oficio o a instancia del propio órgano judicial, en procesos en los que la pretensión afecte sustancialmente a la configuración del derecho fundamental a la protección de datos, lo que se lleva a cabo a través de la reforma que acaba de mencionarse.

XXXI

A la vista de todo lo anterior se informa favorablemente el Anteproyecto de Ley Orgánica sometido al parecer de esta Agencia, si bien deberán tenerse en cuenta las observaciones contenidas en los apartados VI, VII, XVIII, XXIV, XXV y XXVIII de este informe y que se señalan a continuación:

1. La reubicación del artículo 20 del Anteproyecto, que debería incorporarse como último precepto del Capítulo I del Título II, inmediatamente posterior al referido a "categorías especiales de datos".

2. La reubicación del Capítulo II del Título II, que debería ubicarse en el texto con posterioridad a las disposiciones del Título III.

3. La valoración acerca de la necesidad de conservar el artículo 11 del Anteproyecto, al no implicar novedad alguna en relación con el resto del texto o adaptación o aclaración del Reglamento General de Protección de Datos.

4. La modificación consistente en la adición del adverbio "únicamente" al artículo 12.2 del Anteproyecto, que se referiría al tratamiento de "(…) los datos relativos a los empresarios individuales cuando se refieran a ellos **únicamente** en dicha condición (…)".

5. La modificación de la referencia efectuada por el artículo 30.2 al artículo 11 del Anteproyecto en caso de que no sea tomada en consideración la propuesta de reubicación del precepto mencionada en el punto 1.

6. La inclusión en el artículo 46 de un apartado en que se indicase que **los actos dictados por la Agencia española de Protección de Datos agotan la vía administrativa, siendo susceptibles de recurso contencioso-administrativo ante la Audiencia Nacional**.

7. La modificación del artículo 47.6 del Anteproyecto, pasando a tener la siguiente redacción:

> "La Agencia española de Protección de Datos **elaborará su** relación de puestos de trabajo, que **será** aprobada por el Ministerio de Hacienda y Función Pública **a propuesta de la misma. En dicha relación de puestos de trabajo** constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas."

8. La modificación del artículo 48 del Anteproyecto, diferenciando las competencias atribuidas a la Agencia española de Protección de Datos por el propio texto y el reglamento General de Protección de Datos de las otorgadas por otras normas de derecho interno o de la Unión Europea, pasando a tener la siguiente redacción:

> "Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas **en el artículo 57 y las potestades previstas en el artículo 58 del mismo Reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo**.
>
> **Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras Leyes u otras normas de derecho de la Unión Europea."**

9. La clarificación de la norma que regulará la publicidad de las resoluciones de la Agencia Española de Protección de Datos a la que se refiere el artículo 51 del Anteproyecto, que pasaría a tener la siguiente redacción:

> "La Agencia Española de Protección de Datos publicará en la forma que **determine mediante Circular** las resoluciones de su Presidente que declaren haber lugar o no a la atención de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, las que pongan fin

a los procedimientos de reclamación, las que archiven las actuaciones previas de investigación, las que sancionen con apercibimiento a las entidades a que se refiere el artículo 77.1 de esta ley, las que impongan medidas cautelares y las demás que disponga su Estatuto"

10. La supresión del último inciso del párrafo primero del artículo 54 del Anteproyecto.

11. La modificación de artículo 65, estableciendo un régimen de admisión a trámite de las reclamaciones e incorporando en un solo precepto lo dispuesto por los artículos 65 y 66 del Anteproyecto, resultando la redacción del nuevo artículo 65 la siguiente:

"Artículo 65. Iniciación de los procedimientos **y admisión a trámite**

1. Los procedimientos **regulados en este Capítulo se iniciarán cuando se acuerde por la Agencia Española de Protección de Datos la admisión a trámite de la reclamación formulada ante la misma**.

2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos de carácter personal, carezcan manifiestamente de fundamento, sean abusivas o no se aporten elementos que permitan investigar la existencia de una vulneración de los derechos reconocidos.

3. Cuando las reclamaciones no se hayan formulado previamente ante el delegado de protección de datos designado por el encargado o responsable del tratamiento o ante el organismo de supervisión establecido para la aplicación de los códigos de conducta, la Agencia podrá remitírselas**, antes de resolver la admisión a trámite,** a los efectos previstos en los artículos 38 y 39.3.

4. **Igualmente, antes de la admisión a trámite de la reclamación, la Agencia Española de Protección de Datos podrá resolver no iniciar el procedimiento cuando** el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio al afectado en el caso de las infracciones previstas en el artículo 74.

b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

5. Con carácter previo **a la admisión a trámite de la reclamación**, la Agencia Española de Protección de Datos examinará su competencia y determinará el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir o remitirá la reclamación formulada a la Autoridad de control principal que considere competente.

6. La decisión sobre la admisión o inadmisión a trámite, así como la que determine en su caso la remisión de la reclamación a la autoridad de control principal que se estime competente deberá notificarse al reclamante en el plazo de tres meses.

Si no se produjera dicha notificación, se entenderá que el procedimiento se ha iniciado en la fecha en que se cumpliesen tres meses desde que tuvo entrada en la Agencia española de Protección de Datos la reclamación."

12. La modificación del artículo 67.1 como consecuencia de lo propuesto en el punto 11, pasando a tener la redacción siguiente:

"Los plazos máximos de tramitación de los procedimientos y notificación de las resoluciones que los terminen se establecerán mediante real decreto, que no podrá fijar un plazo superior a 18 meses **a contar desde la fecha de admisión a trámite de la reclamación**."

13. La modificación del artículo 69.3, pasando a tener el siguiente tenor:

"**Cuando la reclamación presentada ante la Agencia se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá acordar con anterioridad a la apertura del procedimiento, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado., prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.**"