Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente al Anteproyecto de Ley de Seguridad Privada, 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

El Anteproyecto sometido a informe tiene por objeto, conforme dispone su artículo 1.1 "regular la realización y la prestación por personas físicas o jurídicas, de actividades y servicios de seguridad privada que son contratados, voluntaria u obligatoriamente, por personas físicas o jurídicas, públicas o privadas, para la protección de personas y bienes. Igualmente regula las investigaciones privadas que se efectúen sobre aquéllas o éstos", teniendo estas actividades "la consideración de complementarias y subordinadas respecto de las de seguridad pública", a cuyo efecto se establece un marco más eficiente de coordinación entre los servicios de seguridad privada con los de las Fuerzas y Cuerpos de Seguridad, de los que son complementarios, conforme señala el artículo 1.2.

El texto objeto de informe extiende su actuación, tal y como señala su artículo 3.1 "a las empresas de seguridad privada, al personal de seguridad privada, a los servicios de seguridad privada, a las medidas de seguridad y a los contratos celebrados en éste ámbito", así como, conforme al artículo 3.2 "a los establecimientos obligados a disponer de medidas de seguridad, a los usuarios de los servicios de seguridad privada, a los ingenieros y técnicos de las empresas de seguridad, a las empresas prestadoras de servicios de seguridad de la información y las comunicaciones inscritas en el registro correspondiente, a las centrales de alarma de uso propio y a los centros de formación de personal de seguridad privada".

La Memoria de Impacto Normativo del Anteproyecto y su propia Exposición de Motivos ponen de manifiesto que el régimen contenido en el Anteproyecto introduce importantes modificaciones sobre el previsto en la normativa actualmente vigente, contenida esencialmente en la Ley 23/1992, de 30 de julio, y su desarrollo reglamentario a través del Real Decreto 2364/1994, de 9 de diciembre, pasando a regularse detalladamente las distintas actividades, servicios y medidas de seguridad, que deberán en todo caso desarrollarse como complemento a la garantía de la seguridad ciudadana y quedando sometido el personal que las lleve a cabo a los principios que se establecen en su artículo 30.

Las actividades, servicios, funciones y medidas de seguridad implicarán, desde la perspectiva de la competencia de esta Agencia una multitud de supuestos en los que se procederá al tratamiento de datos de carácter personal, debiendo en tal caso respetarse los principios contenidos en la Ley Orgánica 15/1999 y en su normativa reglamentaria de desarrollo.

En este sentido, si bien es cierto que la Ley puede, de conformidad con lo dispuesto en los artículos 6.1 y 11.2 a) de la Ley Orgánica 15/1999, establecer causas específicas legitimadoras del tratamiento de los datos de carácter personal sin que se haga preciso en tales supuestos recabar el consentimiento de los afectados, debe tenerse en cuenta que tales limitaciones deberán en todo caso resultar respetuosas con el contenido esencial del derecho fundamental, conforme exige el artículo 53.1 de la Constitución. Así lo ha puesto de relieve el Tribunal Constitucional en la Sentencia 17/2013, de 31 de enero, en cuyo fundamento jurídico 4 se señala lo siguiente:

> *"En conclusión, tal como establece nuestra doctrina, es claro que la LOPD no permite la comunicación indiscriminada de datos personales entre Administraciones Públicas dado que, además, estos datos están, en principio, afectos a finalidades concretas y predeterminadas que son las que motivaron su recogida y tratamiento. Por tanto, la cesión de datos entre Administraciones Públicas sin consentimiento del afectado, cuando se cedan para el ejercicio de competencias distintas o que versen sobre materias distintas de aquellas que motivaron su recogida, únicamente será posible, fuera de los supuestos expresamente previstos por la propia LOPD, si existe previsión legal expresa para ello [art. 11.2.a) en relación con el 6.1 LOPD] ya que, a tenor de lo dispuesto en el art. 53.1 CE, los límites al derecho a consentir la cesión de los datos a fines distintos para los que fueron recabados están sometidos a reserva de ley. Reserva legal que, como es obvio, habrá de cumplir con los restantes requisitos derivados de nuestra doctrina- esencialmente, basarse en bienes de dimensión constitucional y respetar las exigencias del principio de proporcionalidad- para poder considerar conforme con la Constitución la circunstancia de que la norma legal en cuestión no contemple, por tanto, la necesidad de contar con el consentimiento del afectado para autorizar la cesión de datos."*

De este modo deberá verificarse si dicha habilitación resulta coherente con los principios de protección de datos y, particularmente, con los consagrados en el artículo 4 de la Ley Orgánica 15/1999. En este sentido, el artículo 4.1 de la Ley Orgánica 15/1999 dispone que "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido", añadiendo el artículo 4.2 que "los datos de

carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos".

Hecha esta consideración previa, las cuestiones relacionadas con la aplicación de las previsiones de la Ley Orgánica 15/1999 en el ámbito desarrollado por el Anteproyecto sometido a informe que deberán ser objeto de análisis específico se refieren esencialmente a los tratamientos que serán llevados a cabo en los ámbitos de la videovigilancia y la actividad de los detectives privados, así como al tratamiento de datos de carácter personal que se derivará del cumplimiento de los requisitos que el Anteproyecto establece para el ejercicio de funciones de seguridad privada o como consecuencia de la comunicación de datos que se llevará a cabo por parte de las empresas de seguridad privada a las Fuerzas y Cuerpos de seguridad y el marco de cooperación establecido entre éstas y aquéllas. Además junto con estas cuestiones será preciso hacer referencia a otras que revisten especial importancia en lo referente al ámbito de aplicación de la normativa de seguridad privada, que afectará a la propia legitimación para la realización de determinados tratamientos de datos en este ámbito y, finalmente, el análisis del régimen sancionador establecido en el Anteproyecto, a fin de evitar posibles supuestos de concurrencia en la aplicación de las normas de protección de datos y de seguridad privada.

II

Dentro de las materias a las que acaba de hacerse referencia debe comenzarse el análisis del Anteproyecto, por motivos de sistemática, con la problemática que pudiera derivarse de la delimitación del ámbito de aplicación del Anteproyecto y la delimitación de los supuestos, actividades, servicios y medidas de seguridad privada que el mismo parece reservar en exclusiva a determinados colectivos.

Como ya se ha señalado la delimitación de este ámbito de aplicación resulta especialmente relevante en lo que afecta a la aplicación de la normativa de protección de datos, dado que podría influir en la fijación de los criterios que determinan la legitimación para llevar a cabo determinados tratamientos de datos relacionados con actividades que podrían incluirse en el marco establecido en el Anteproyecto.

En este punto, debe traerse a colación la evolución del parecer de esta Agencia en relación con un tratamiento en que la vinculación entre la normativa de protección de datos y la relacionada con el desempeño de actividades de seguridad privada resulta especialmente concurrente, cual es el de la videovigilancia. Por ello, y sin perjuicio del posterior análisis de las normas específicas contenidas en el Anteproyecto en relación con estas medidas, debe ahora hacerse una escueta referencia a la citada evolución.

Así, debe recordarse que en un primer momento, y tras la adopción por esta Agencia de la Instrucción 1/2006, de 8 de noviembre, el parecer de esta Agencia fue el de considerar que el tratamiento de imágenes a través de sistemas de videovigilancia se encontraba amparado por lo dispuesto en el artículo 6.1 de la Ley Orgánica 15/1999, en el sentido de existir una norma con rango de Ley habilitante del tratamiento, en conexión con la Ley de Seguridad Privada, siempre que la instalación de las videocámaras se hubiera llevado a cabo cumpliendo los requisitos legalmente establecidos y reducidos esencialmente a la contratación de una empresa de seguridad privada y la comunicación del correspondiente contrato que incorporase estas medidas al Ministerio del Interior.

Posteriormente, en informe de 25 de enero de 2010 se analizó por esta Agencia si dicho parecer debía considerarse modificado como consecuencia de la entrada en vigor de la Ley 25/2009, de 27 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios, alcanzando el citado informe las siguientes conclusiones:

> *"Primera; la Ley permite la instalación y mantenimiento de sistemas de seguridad, por cualquier prestador de servicios, por lo que se legitima el tratamiento de las imágenes derivados de estos dispositivos, sin necesidad de obtener el consentimiento de los interesados, al amparo del artículo 11.2 a) de ley Orgánica 15/1999 y el artículo 10.2 a) del Reglamento de desarrollo de la misma.*
>
> *Segunda; Para la instalación y mantenimiento de los dispositivos de seguridad, no se exige como regla general, el cumplimiento de los requisitos formales, exigidos hasta la entrada en vigor de la Ley 25/2009, sino que podrá instalarlos y mantenerlos cualquier prestador de servicios.*
>
> *Tercera; Sólo será necesario que se cumplan los requisitos exigidos tanto en la Ley de Seguridad Privada como en su Reglamento, y que hasta ahora debían de cumplirse en todos los casos; esto es, empresa de seguridad debidamente autorizada por el Ministerio del Interior, previa inscripción en su Registro y notificación del contrato, cuando el dispositivo de seguridad esté conectado a una central de alarmas.*
>
> *Cuarto; Resulta necesario seguir cumpliendo con todos los requisitos previstos en la Ley Orgánica 15/1999 y su normativa de desarrollo."*

Finalmente, la resolución de esta Agencia de 20 de diciembre de 2012, dictada en recurso de reposición presentado por Renfe operadora contra resolución de esta Agencia por la que se declaraba la infracción de la Ley Orgánica 15/1999 como consecuencia del tratamiento de imágenes por parte

de la misma en las zonas de aparcamiento de determinadas estaciones de ferrocarril tuvo en consideración el efecto derivado de la sentencia del tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, por la que se declaraba el efecto directo del artículo 7 f) de la Directiva 95/46/CE y la sentencia del Tribunal Supremo de 8 de febrero de 2012, que resuelve el recurso en cuyo ámbito se planteó la cuestión prejudicial resuelta por la sentencia anteriormente mencionada. En dicha resolución, resumidamente se señala lo siguiente en cuanto a la legitimación para el tratamiento:

> *"(…) la aplicación de las causas de legitimación analizadas en el punto anterior a los supuestos de captación de imágenes a través de sistemas de videovigilancia implica la posible concurrencia de dos supuestos diferenciados*
>
> *Un primer caso será el de instalación de los citados dispositivos en los denominados "espacios públicos" a los que se refiere la Ley Orgánica 4/1997. En estos supuestos, el tratamiento de los datos será legítimo, por encontrarse amparado en una norma con rango de Ley (artículo 6.1 de la LOPD), siempre y cuando se cumplan los requisitos exigidos por la citada Ley Orgánica para que la instalación pueda tener lugar y únicamente cuando se cumplan efectivamente tales exigencias.*
>
> *En los restantes supuestos, y siempre que no sea de aplicación la excepción doméstica contenida en el artículo 2.2 a) de la LOPD, la legitimación para el tratamiento de imágenes con fines de videovigilancia para preservar la seguridad de las instalaciones únicamente podrá venir fundada en lo dispuesto en el artículo 7 f) de la Directiva 95/46/CE, al no ser posible recabar el consentimiento de las personas cuyas imágenes sean objeto de captación, ni existir una norma con rango de Ley que habilite el tratamiento ni ser aplicables las excepciones establecidas en el artículo 6.2 de la LOPD."*

El artículo 5.1 del Anteproyecto sometido a informe enumera las actividades de seguridad privada, incluyendo entre las mismas "la vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados, así como de las personas que pudieran encontrarse en los mismos" (apartado a), "la instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia" (apartado f), "la explotación de centrales para la recepción, verificación y transmisión de las señales de alarmas, así como la monitorización de cualesquiera señales de dispositivos auxiliares para la seguridad de personas, de bienes muebles o inmuebles o de cumplimiento de medidas impuestas, y la comunicación a las Fuerzas y Cuerpos de Seguridad en todos estos casos" (apartado g) y "la investigación privada" (apartado i).

Por su parte, el artículo 6.1 del Anteproyecto señala que "quedan fuera del ámbito de aplicación de esta ley y podrán ser desarrolladas por las empresas de seguridad privada, sin perjuicio de la normativa específica que pudiera resultar de aplicación, especialmente en lo que se refiere a la homologación de productos" las actividades de "fabricación, comercialización, venta o entrega de equipos técnicos de seguridad electrónica, así como la instalación o mantenimiento de dichos equipos siempre que no incluyan la prestación de servicios de conexión con centrales de alarma o centros de control o de videovigilancia" (apartado b) y "de seguridad informática, entendidas como el conjunto de medidas encaminadas a proteger los sistemas de información a fin de garantizar la confidencialidad, disponibilidad e integridad de la misma o del servicio que aquéllos prestan. Reglamentariamente podrán imponerse requisitos específicos para garantizar la fiabilidad y seguridad a las empresas que no sean de seguridad privada que presten este tipo de actividades (apartado e).

A su vez, los apartados 4 y 5 de este precepto disponen lo siguiente:

"4. Los prestadores de servicios y las filiales de empresas de seguridad privada que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, siempre que no incluyan la prestación de servicios de conexión con centrales de alarmas o con centros de control o de videovigilancia, quedan excluidos de la legislación de seguridad privada.

5. Las empresas de seguridad privada que se dediquen a la instalación o mantenimiento de aparatos, dispositivos y sistemas de seguridad que no incluyan la conexión a centrales de alarma o a centros de control o de videovigilancia, sólo están sometidas a la normativa de seguridad privada en lo que se refiere a las actividades y servicios de seguridad privada para las que se encontrasen autorizadas."

Finalmente, conforme al artículo 7 del Anteproyecto "No están sujetas a esta ley las actuaciones de autoprotección, entendidas como el conjunto de cautelas o diligencias que se puedan adoptar individual o colectivamente que ejecuten por sí y para sí mismos de forma directa los interesados, estrictamente dirigidas a la protección de su persona o del propio entorno privado, y cuya práctica o aplicación no conlleve contraprestación alguna ni suponga algún tipo de servicio de seguridad privada a terceros".

De lo dispuesto en los preceptos antedichos parece desprenderse que, sin perjuicio de su posible desarrollo por parte de empresas de seguridad privada, las actividades descritas en el artículo 6 del Anteproyecto y las relacionadas con la autoprotección a las que se refiere el artículo 7 quedarían excluidas del ámbito de aplicación de la Ley de Seguridad Privada, aunque no se deduce claramente de estas normas si dichas actividades deben ser o no consideradas actividades de seguridad privada.

Ello resulta relevante, por cuanto el artículo 38 del Anteproyecto establece que “Los servicios de seguridad privada se prestarán únicamente por empresas de seguridad privada, inscritas y autorizadas para la actividad relativa a los mismos, y por personal de seguridad privada, legalmente habilitado para el ejercicio de las funciones referidas a dichos servicios”. De este modo, si pudiera considerarse que servicios tales como los referidos a la videovigilancia, incluso en los casos en que no exista conexión a centrales receptoras de alarma, o seguridad informática, en los términos referidos por el Anteproyecto, aun cuando se establecieran con fines de autoprotección pudieran ser considerados como servicios de seguridad privada, nos encontraríamos con la contradicción de que lo excluido de la Ley en sus artículos 6 y 7 aparecería sometido a los trámites administrativos previstos en la misma por aplicación de lo señalado en el artículo 38.

Esta Agencia considera que una interpretación sistemática de la norma podría permitir considerar que el artículo 6 del Anteproyecto tiene por finalidad señalar aquellos servicios que sin ser considerados a los efectos del mismos como seguridad privada, podrán no obstante desarrollarse por la empresas de seguridad privada, aunque en competencia con cualesquiera otros operadores existentes en el mercado y que cumplan los requisitos para el desarrollo de las actividades vinculadas con dichos servicios. Del mismo modo, del artículo 7 se desprende que cuando no exista una intervención efectiva de las empresas de seguridad privada en el desarrollo de los servicios de autoprotección no cabrá exigir el cumplimiento de los requisitos legales exigidos por el texto sometido a informe.

No obstante, sería deseable que estas conclusiones, de ser exactas, consten claramente en el Anteproyecto, por cuanto una interpretación restrictiva de sus disposiciones podría llevar aparejadas consecuencias que incluso afectarían a la actividad y competencias de esta Agencia, toda vez que, por ejemplo, las actividades de seguridad informática, que incluirían el cumplimiento de las medidas de seguridad exigidas por el artículo 9 de la Ley Orgánica 15/1999 y el Título VIII del Reglamento que la desarrolla, podría tener que ser prestadas por empresas de seguridad privada, siendo similar la limitación para la instalación de dispositivos de autoprotección, en particular de videovigilancia, cuando ya se ha indicado que, sin perjuicio del cumplimiento de la normativa de seguridad privada cuando esta sea de aplicación, la legitimación para el establecimiento de tales dispositivos se fundará en el interés legítimo del interesado, siempre que el mismo prevalezca sobre el derecho a la protección de datos de las personas cuyas imágenes son objeto de captación.

Ello resulta especialmente relevante en relación con los servicios de seguridad informática a los que se refiere el artículo 6.1 d), dado que los mismos pueden entrar en completa concurrencia con los que es su caso pudieran ser contratados por los responsables de los ficheros para el cumplimiento del deber de seguridad establecido en las normas de protección

de datos o incluso para el cumplimiento de las obligaciones de notificación de fallos de seguridad que tengan la consideración de "violación de datos personales" en los supuestos en los que la normativa sectorial específica impone este deber, como sucede en los casos previstos en el artículo 34 de la Ley 32/2003, de 3 de noviembre general de Telecomunicaciones, en la redacción dada al mismo por el Real decreto-Ley 13/2012, de 30 de marzo.

Por todo ello, se considera por esta Agencia **que debería clarificarse en el artículo 6 del Anteproyecto que las actividades a las que se refiere el apartado 1 podrán ser llevadas a cabo además de por las empresas de seguridad privada por otros operadores que carezcan de esa naturaleza, en régimen de libre competencia**, a fin de delimitar con claridad las causas legitimadoras del tratamiento de datos derivado de la realización de tales actividades o la implantación de las medidas de autoprotección previstas en el artículo 7.

Dentro de las disposiciones generales a las que ahora se está haciendo referencia debe hacerse mención igualmente en este informe de los dispuesto en el artículo 8.5 del Anteproyecto, cuyos apartados b) y c) establecen la prohibición de las empresas y el personal de seguridad privada de "ejercer ningún tipo de control sobre opiniones políticas, sindicales o religiosas, o sobre la expresión de tales opiniones, ni crear ni mantener ficheros, automatizados o no, de datos de carácter personal" y "comunicar a terceros, salvo a las autoridades judiciales y policiales para el ejercicio de sus respectivas funciones, cualquier información que conozcan en el desarrollo de sus servicios y funciones sobre sus clientes o personas relacionadas con éstos, así como sobre los bienes y efectos de cuya seguridad estuvieren encargados".

En particular, la primera de las prohibiciones trae causa de lo establecido en el artículo 16.1 de la Constitución, pero ya resulta expresamente prohibido por la Ley Orgánica 15/1999, según cuyo artículo 7.1 "de acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias", aclarando el artículo 7.2 que "sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias".

Si bien la regla contenida en el artículo 8.5 b) del Anteproyecto supone una clarificación de la establecido en los artículos precedentes, **sería conveniente homogeneizar ambas normas, reemplazando la expresión "ni crear ni mantener ficheros, automatizados o no, de datos de carácter personal" por "ni proceder al tratamiento, automatizado o no de datos relacionados con la ideología, afiliación sindical, religión o creencias"**.

III

En cuanto a los requisitos y trámites legalmente exigidos para el desempeño de actividades reguladas por el Anteproyecto, debe hacerse en primer lugar referencia a las normas reguladoras de las exigencias legales para el ejercicio de la actividad de seguridad privada.

En este sentido, el artículo 19.1 del texto sometido a informe enumera los requisitos generales exigibles a las empresas de seguridad privada para la autorización e inscripción en el Registro Nacional de Seguridad Privada o en el correspondiente registro autonómico y el desarrollo de servicios de seguridad privada, entre los que se encuentra "no haber sido condenadas mediante sentencia firme por delitos de insolvencia punible, contra la Hacienda Pública, contra la Seguridad Social o contra los derechos de los trabajadores, salvo que se hubieran cancelado sus antecedentes penales. En el caso de las personas jurídicas, este requisito será aplicable a los administradores de hecho o de derecho y representantes, que, vigente su cargo o representación, no podrán estar incursos en la situación mencionada por actuaciones realizadas en nombre o a beneficio de dichas personas jurídicas" (apartado f).

Por su parte, en cuanto a los representantes de dichas empresas, el artículo 21.2 e) del Anteproyecto establece como límite a los mismos "No haber sido administrador de hecho o de derecho o apoderado general, en los diez años anteriores, en una empresa que haya sido declarada en concurso calificado como culpable, o condenada mediante sentencia firme por delitos de insolvencia punible, contra la Hacienda Pública, contra la Seguridad Social o contra los derechos de los trabajadores".

Finalmente, respecto del personal de seguridad, el artículo 28.1 h) les impone "no haber sido condenado por intromisión ilegítima en el ámbito de protección del derecho al honor, a la intimidad personal y familiar o a la propia imagen, vulneración del secreto de las comunicaciones o de otros derechos fundamentales en los cinco años anteriores a la solicitud".

Dentro de los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, el artículo 197.2 del Código Penal tipifica el delito que comete el que "sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero", aplicándole la pena prevista en el artículo 197.1. Asimismo, el artículo 197.3 se refiere al que "por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del

mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo", señalando que "será castigado con pena de prisión de seis meses a dos años".

Añade el párrafo segundo de este precepto que "cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis , los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33". Finalmente, los apartados 4 y siguientes del artículo 197 establecen determinadas reglas especiales en atención a la naturaleza de los datos o la intencionalidad de la conducta.

Pues bien, esta Agencia se muestra plenamente conforme con que la condena por la comisión de estos delitos impida el desempeño de funciones propias del personal de seguridad. Ahora bien, cabría plantearse si no debería ser exigibles este requisito en los mismos términos para las propias empresas, dado que el artículo 197.3 se refiere expresamente a la posible comisión del delito por personas jurídicas. En este sentido, **sería conveniente que se estableciese para las empresas de seguridad y sus representantes la misma limitación establecida para el personal de seguridad para poder ejercer las actividades de seguridad privada, quedando excluido tal ejercicio en caso de condena por la comisión de los delitos tipificados por el artículo 197 del Código Penal**.

IV

Por otra parte, en relación con los requisitos para el ejercicio de la actividad y la implantación de medidas de seguridad privada, el artículo 9 del Anteproyecto sometido a informe dispone en su apartado 1 que "no podrá prestarse ningún tipo de servicio de seguridad privada que no haya sido previamente contratado y, en su caso, autorizado", añadiendo el apartado 2 que "de acuerdo con lo que reglamentariamente se determine, los contratos de prestación de los distintos servicios de seguridad privada deberán, en todo caso, consignarse por escrito y comunicarse al Ministerio del Interior o, en su caso, al órgano autonómico competente con antelación a la iniciación de los mismos".

A su vez, el artículo 11 del Anteproyecto regula el Registro Nacional de Seguridad Privada y registros autonómicos, disponiendo en su apartado 1 que las autorizaciones, habilitaciones, comunicaciones o, en su caso, declaraciones responsables de las empresas de seguridad privada, de los despachos de detectives privados, del personal de seguridad privada, de los contratos, de los servicios de seguridad privada, de los centros de formación, de las centrales de alarma de uso propio, así como las sanciones impuestas y cuantos datos sean necesarios para las actuaciones de control y gestión de la seguridad privada,

se inscribirán de oficio en el Registro Nacional de Seguridad Privada del Ministerio del Interior.

Por su parte, los apartados 2 a 4 establecen el procedimiento de colaboración entre el Registro nacional y los registros que pudieran ser creados por las Comunidades Autónomas competentes en la materia. Así se prevé que "en el referido Registro, además de la información correspondiente a las empresas de seguridad privada que en el mismo se inscriban, se incorporará la relativa a las empresas de seguridad privada inscritas en los registros de las comunidades autónomas con competencia en la materia. Igualmente se recogerán los datos de las empresas que realicen actividades de seguridad de la información y las comunicaciones que voluntariamente deseen inscribirse a efectos de homologación, en la forma que reglamentariamente se determine", aclarando el artículo 11.3 que "a efectos de lo dispuesto en el apartado anterior, los órganos competentes de las mencionadas comunidades autónomas deberán comunicar al Registro Nacional de Seguridad Privada los datos de las inscripciones y anotaciones que efectúen sobre las empresas de seguridad privada que inscriban y autoricen, así como de sus modificaciones y cancelaciones" y en el artículo 11.4 que "las autoridades responsables del Registro Nacional y de los registros autonómicos establecerán los mecanismos de colaboración necesarios para permitir su interconexión, la determinación coordinada de los sistemas de numeración de las empresas de seguridad privada y el acceso a la información registral contenida en los mismos, para el ejercicio de las respectivas competencias".

En cuanto a su publicidad se dispone que "dichos registros serán públicos exclusivamente en cuanto a los asientos referentes a la denominación o razón social, domicilio, número de identificación fiscal y actividades en relación con las cuales está autorizada para prestar servicios de seguridad privada. Respecto del personal de seguridad privada serán públicos sus datos personales y las habilitaciones de que disponga", previéndose la regulación de la organización y funcionamiento del Registro en el desarrollo reglamentario del Anteproyecto.

Las normas que se han reproducido plantean diversos problemas de diversa complejidad, por cuanto, en primer lugar, existirá un tratamiento por los correspondientes registros de datos de carácter personal, no sólo de los datos relacionados con las empresas de seguridad privada, sino como se analizará de sus clientes, que debe encontrar amparo legal en las previsiones de la Ley Orgánica y respetar el contenido esencial del derecho fundamental a la protección de datos. Asimismo, de estas normas se desprende la existencia de dos tipos de cesiones: la que tendrá lugar entre las Administraciones competentes como consecuencia de la interconexión de los registros Nacional y autonómicos que pudieran existir y, en segundo lugar, la relativa a su publicidad, debiendo estas cesiones encontrar igualmente amparo en lo dispuesto en la Ley Orgánica 15/1999 y su normativa de desarrollo.

Las cuestiones relacionadas con las cesiones a las que se refiere el artículo 11 plantean una menor complejidad, por lo que haremos referencia a las mismas con carácter previo. Así, en cuanto a la interconexión entre las administraciones que resulten competentes y la consiguiente cesión al registro nacional de los datos incluidos en el Registro, el artículo 21.1 de la Ley Orgánica 15/1999 dispone que "Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos".

En este mismo sentido, el artículo 10.4 c) del reglamento de desarrollo de la Ley Orgánica dispone que "la cesión entre Administraciones Públicas cuando concurra uno de los siguientes supuestos (…) la comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias".

De este modo, siempre que la intercomunicación entre los registros nacional y autonómicos únicamente permita el acceso por éstos últimos a la información relativa a las empresas sobre las que las mismas puedan ejercer sus competencias la cesión se encontrará amparada por la Ley Orgánica 15/1999.

En cuanto a la cesión de datos derivada de su publicidad, ya se ha indicado que el establecimiento de una habilitación legal para la cesión de datos exige el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999 y particularmente el respeto de los principios contenidos en su artículo 4, que configura, entre otras normas, el contenido esencial del derecho a los efectos del artículo 53.1 de la Constitución. Así, deberá particularmente analizarse si la cesión derivada de la publicidad de los datos cumple lo exigido por el artículo 4.1 de la Ley Orgánica 15/1999, a cuyo tenor "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

Al propio tiempo, en cuanto a la información pueda referirse a personas jurídicas o a datos de empresarios individuales relacionados exclusivamente con su actividad mercantil, debe recordarse que los artículos 2.2 y 2.3 del reglamento de desarrollo de la Ley Orgánica 15/1999 excluyen el tratamiento de sus datos de la normativa de protección de datos.

En cuanto al personal de las empresas de seguridad, el Anteproyecto señala que la publicidad se limitará a "sus datos personales y las habilitaciones de que disponga".

A nuestro juicio, la finalidad de prevención del intrusismo, reflejada en numerosos lugares de la Exposición de motivos y la Memoria de impacto normativo del Anteproyecto, así como la reserva de numerosos servicios en exclusiva al personal habilitado justificarían la divulgación de la información que identifique al personal de seguridad y las habilitaciones de que el mismo gozase.

Ahora bien, el Anteproyecto se refiere a "datos personales", siendo así que dicho término se refiere a un concepto jurídico mucho más amplio que el citado, por cuanto el artículo 3 a) de la Ley Orgánica 15/1999 define a los mismos como "cualquier información concerniente a personas físicas identificadas o identificables", lo que excedería de la mera referencia a datos identificativos, que es lo que parece desprenderse del tenor del texto.

Por este motivo, **debería reemplazarse la expresión "datos personales" del artículo 11.5 del Anteproyecto por "datos meramente identificativos"**, a fin de garantizar el cumplimiento del citado principio de proporcionalidad contenido en el artículo 4.1 de la Ley Orgánica 15/1999.

Junto a estos supuestos ya se señaló que del artículo 11 se deriva el tratamiento por parte del registro nacional, y cuando existan, de los registros autonómicos, en su caso, de una gran pluralidad de datos que habrán de ser inscritos en aquéllos. Así, ya se ha dicho que el artículo 11.1 del Anteproyecto se refiere a la inscripción y depósito en el Registro de, en primer lugar, "las autorizaciones, habilitaciones, comunicaciones o, en su caso, declaraciones responsables de las empresas de seguridad privada, de los despachos de detectives privados, del personal de seguridad privada, de los contratos, de los servicios de seguridad privada, de los centros de formación, de las centrales de alarma de uso propio, así como las sanciones impuestas y cuantos datos sean necesarios para las actuaciones de control y gestión de la seguridad privada". Como ya se ha indicado será preciso que el tratamiento de estas informaciones pueda ser considerado adecuado, pertinente y no excesivo en relación con las finalidades del Registro para que pueda considerarse que la habilitación derivada del artículo 11.1 del Anteproyecto resulta ajustada a lo dispuesto en la Ley Orgánica 15/1999.

Como puede comprobarse de la lectura del artículo 11.1 se desprende que la mayor parte de los datos que serán incorporados al Registro nacional regulado por el mismo se encuentran relacionados directamente con la habilitación conferida a las empresas de seguridad, incluyendo los despachos de detectives privados, para que dichas entidades lleven a cabo sus funciones, evitando, por una parte, el intrusismo en el ejercicio de estas actividades, como finalidad esencialmente perseguida por la norma y garantizando, por otra, el adecuado control de la actividad encomendado a las Administraciones Públicas, al que se hará referencia en lugares posteriores de este informe.

No obstante, el artículo 11.1 incorpora una información que puede dar lugar al tratamiento de una serie de datos de carácter personal vinculados con los clientes que solicitan la adopción de las medidas o la solicitud de los servicios regulados por el Anteproyecto, cual es la referida a los contratos celebrados por las empresas de seguridad privada y despachos de detectives privados. Respecto de dicha información es preciso efectuar una análisis más detallado acerca del cumplimiento del principio de proporcionalidad, toda vez que, como se ha dicho, la información no se referirá únicamente a la actividad de las empresas que deben contar con la correspondiente habilitación o autorización, sino que se extiende también a datos relacionados con la actividad e incluso características personales de los clientes, así como en determinados casos de terceras personas.

De este modo, sería posible la incorporación al registro nacional de datos que exceden de los necesarios para el adecuado ejercicio de las competencias de las Administraciones Públicas o del control del intrusismo en esta actividad, pudiendo así describirse las actividades o dependencias del cliente que solicita la prestación de determinados servicios o la adopción de ciertas medidas de seguridad; asimismo, es posible que incluso esta información pueda referirse a efectos del citado cliente que hayan de ser objeto de protección o a informaciones de aquél necesarias para desarrollar adecuadamente actividades de vigilancia, que podrían incluso incorporar datos especialmente protegidos.

En el mismo sentido, los contratos celebrados por los despachos de detectives privados, a tenor de las funciones atribuidas a los mismos por los artículos 37 y 49 del Anteproyecto pueden no sólo incorporar información sobre el propio cliente, que justifica la realización en su caso de actividades de seguimiento y la realización por estos despachos del juicio de ponderación exigido por el artículo 49.2 del Anteproyecto, sino también información referida a la persona física que en su caso sea objeto de la investigación, especialmente en virtud de lo dispuesto en el artículo 37.1 a) del texto sometido a informe, dado que los servicios pueden consistir conforme a dicho precepto en la obtención de información y pruebas sobre conductas y hechos privados.

A nuestro juicio, las informaciones a las que se refieren los dos párrafos precedentes pueden resultar excesivas en relación con las finalidades propias del Registro, sin perjuicio de lo que se señalará posteriormente en relación con el acceso a los datos con fines de inspección. Por este motivo sería necesario que el Anteproyecto sometido a informe estableciese alguna cautela que permitiese minimizar los datos relativos a la contratación de los servicios y medidas de seguridad privada que serán incorporados al Registro. De este modo, debería hacerse constar que los contratos únicamente incorporarán los datos mínimos necesarios para la identificación, a lo sumo, del cliente que solicita la prestación de los servicios o la adopción de las medidas y los concretos servicios o medidas contratados.

Lógicamente, la propuesta realizada no podría incluirse en el artículo 11.1 sino que debería constar en el artículo 9, que es el relativo a la contratación de los servicios. Como se ha dicho con anterioridad, el artículo 9.2 impone el deber de consignación escrita del contrato y de comunicación del mismo al Ministerio del Interior. El cumplimiento de la propuesta señalada podría llevarse a cabo **indicando en el artículo 9 del Anteproyecto que la información suministrada será comunicada a través de los modelos que se adopten reglamentariamente que no contendrán más datos que los relativos a la identificación del cliente y las medidas o servicios objeto de contratación, sin especificar más datos de carácter personal y, en particular los de terceros distintos de los del cliente y la prestadora de los servicios**.

V

Dentro de la actividad objeto de regulación por el Anteproyecto cabe igualmente hacer referencia a la cesión de información que se producirá desde las entidades de seguridad privada a las fuerzas y cuerpos de seguridad. Esta cesión de datos puede traer causa de dos fundamentos distintos: el cumplimiento del principio de coordinación y cooperación con las citadas fuerzas y cuerpos y el ejercicio por los órganos competentes de las funciones de supervisión, inspección y control de las actividades llevadas a cabo por las entidades sometidas al régimen del Anteproyecto.

En cuanto al principio de coordinación, el artículo 1.2 del Anteproyecto dispone que “esta ley, en beneficio de la seguridad pública, establece el marco para la más eficiente coordinación de los servicios de seguridad privada con los de las Fuerzas y Cuerpos de Seguridad, de los que son complementarios”.

De este modo, el artículo 4 c) consagra como uno de los fines de la seguridad privada “complementar el monopolio de la seguridad que corresponde al Estado, integrando funcionalmente sus medios y capacidades como un recurso externo de la seguridad pública”.

En este marco, el artículo 8.2 establece que “los servicios de seguridad privada colaborarán, en todo momento y lugar, con las Fuerzas y Cuerpos de Seguridad, con sujeción a lo que éstas puedan disponer en relación con la ejecución material de sus actividades”, añadiendo el artículo 8.3 el principio esencial de que “de conformidad con lo dispuesto en la legislación de Fuerzas y Cuerpos de Seguridad, las empresas y el personal de seguridad privada tendrán especial obligación de auxiliar y colaborar, en todo momento, con éstas en el ejercicio de sus funciones, de prestarles su colaboración y de seguir sus instrucciones”.

En cumplimiento de este deber de colaboración, el Anteproyecto establece diversos deberes de colaboración que implicará cesiones de datos

de carácter personal. Así, en primer lugar, el artículo 14.2 del texto sometido a informe dispone que “las empresas y el personal de seguridad privada deberán comunicar a las Fuerzas y Cuerpos de Seguridad competentes, tan pronto como sea posible, cualesquiera circunstancias o informaciones relevantes para la prevención, el mantenimiento o restablecimiento de la seguridad ciudadana, así como todo hecho delictivo de que tuviesen conocimiento en el ejercicio de su actividad o funciones, poniendo a su disposición a los presuntos delincuentes, así como los instrumentos, efectos y pruebas relacionadas con los mismos”.

Por otra parte, el artículo 15.1 del Anteproyecto dispone que “se autorizan las cesiones de datos que se consideren necesarios para contribuir a la salvaguarda de la seguridad ciudadana, así como la conexión de los servicios de las Fuerzas y Cuerpos de Seguridad a los sistemas instalados por las empresas de seguridad privada que permitan la comprobación de las informaciones en tiempo real”.

En cuanto a la primera de las normas citadas, que exige la existencia de indicios de comisión de un delito o de una vulneración de las previsiones establecidas en la normativa de seguridad ciudadana cabe considerar que la habilitación legal establecida resulta congruente con el contenido del derecho fundamental a la protección de datos.

La previsión del artículo 15.1 presenta una mayor complejidad, puesto que de la misma parece derivarse el establecimiento de un sistema continuado de acceso a la información contenida en los sistemas, que podría resultar excesiva a la luz de los principios contenidos en la Ley Orgánica 15/1999.

En este sentido, cabe recordar que el artículo 22.2 de la Ley Orgánica prevé que “La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad”. De este modo, un acceso permanente a la información obrante en los sistemas excedería de la finalidad a la que ahora se está haciendo referencia, por cuanto resultaría irrelevante la existencia o no del peligro real y grave mencionado o la exigencia de perseguibilidad del delito.

El artículo 15.2 del Anteproyecto dispone, no obstante, que “el tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de esta ley se someterán a lo dispuesto en la normativa de protección de datos de carácter personal”. De este modo, el propio texto sometido a informe parece tener por objetivo una compatibilización de los principios derivados de la necesaria garantía de la

seguridad ciudadana y los consagrados por la normativa de protección de datos.

Ello se lograría si el acceso previsto, sin perjuicio del establecimiento de sistemas que lo pudieran permitir el línea, se realizase en relación con solicitudes concretas de acceso o en caso de que pudiera constar de algún modo la necesidad de acceso a la información, de forma que la misma no se produzca de forma continuada y a cualquier sistema, sino en virtud de una necesidad concreta derivada de lo dispuesto en el artículo 22.2 de la Ley Orgánica 15/1999.

Ello haría precisa una **modificación en la dicción del artículo 15.1 del Anteproyecto** a fin de hace constar la circunstancia mencionada, estableciendo que "se autorizan las cesiones de datos que se consideren necesarios para contribuir a la salvaguarda de la seguridad ciudadana, **así como el acceso por parte** de las Fuerzas y Cuerpos de Seguridad a los sistemas instalados por las empresas de seguridad privada que permitan la comprobación de las informaciones en tiempo real **cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales**".

Por otra parte, el artículo 14.3 del Anteproyecto dispone que "las Fuerzas y Cuerpos de Seguridad podrán facilitar al personal de seguridad privada, en el ejercicio de sus funciones, informaciones que faciliten su evaluación de riesgos y consiguiente implementación de medidas de protección", lo que podría implicar una comunicación al personal de seguridad privada de datos de carácter personal. A ello se añade que el artículo 15 del texto sometido a informe, que parece referirse al acceso a los datos de las empresas de seguridad privada por las fuerzas y cuerpos de seguridad lleva por rúbrica "intercambio de información", lo que parece implicar una posible cesión de datos por las fuerzas y cuerpos de seguridad a las entidades que desarrollan funciones de seguridad privada.

Debe nuevamente tenerse en cuenta que las fuerzas y cuerpos de seguridad pueden proceder al tratamiento de los datos con fines de investigación criminal en el marco establecido en el artículo 22.2 de la Ley Orgánica 15/1999, lo que limita igualmente los supuestos en los que dichas informaciones podrían ser igualmente objeto de comunicación a quienes colaboren con aquéllas en el mantenimiento de la seguridad ciudadana. De este modo, el Anteproyecto no podría amparar una cesión genérica de datos por una finalidad tan amplia como la evaluación de riesgos y consiguiente implementación de medidas de protección a la que se refiere el artículo 14.3, debiendo dicha cesión fundarse precisamente en la existencia de un peligro real y grave para la seguridad de las personas o bienes objeto de protección por las empresas de seguridad privada o la existencia de indicios de la comisión de un ilícito penal contra esa persona y bienes.

Por este motivo, **sería conveniente modificar el tenor del artículo 14.1 sometiendo la cesión de los datos a las empresas de seguridad privada a los presupuestos contenidos en el artículo 22.2 de la Ley Orgánica 15/1999, sin perjuicio de que efectivamente la consecuencia de la cesión sea, lógicamente, la planificación de medidas de seguridad reforzadas como consecuencia de la existencia de ese peligro real y grave o de indicios de la comisión de un delito**.

En todo caso, y **en cuanto a la rúbrica del artículo 15, dado que el mismo se refiere únicamente a las cesiones de datos por parte de las fuerzas y cuerpos de seguridad, debería reemplazarse la expresión "intercambio de información" por "acceso a la información por las Fuerzas y Cuerpos de seguridad".**

Por último, dentro de los artículos 14 y 15 del Anteproyecto, el artículo 15.3 dispone que "la comunicación de buena fe de información a las Fuerzas y Cuerpos de Seguridad por las empresas y el personal de seguridad privada no constituirá vulneración de las restricciones sobre divulgación de información impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa".

A nuestro juicio, debe tenerse en cuenta que la comunicación citada deberá someterse a una serie de requisitos, que se han ido señalando en este apartado del presente informe. Al propio tiempo, esta Agencia considera que la inclusión de una causa de exculpación general como la mencionada en relación con la aplicación de cualquier norma legal, reglamentaria o administrativa, pudiera resultar excesiva, siendo así que debería ser el órgano competente para la aplicación de esa norma quien hubiera de valorar si efectivamente concurren las circunstancias que permitan excluir la culpabilidad. En otro caso, las entidades podría añadir a lo previsto en la norma a la que ahora se hace referencia la invocación de la confianza legítima en que un requerimiento de información por parte de las fuerzas y cuerpos de seguridad es siempre respetuoso con las normas, lo que garantizaría la aplicación de la regla de la buena fe en cualquier supuestos de cesión, sin que se entrase en ningún caso a valorar las circunstancias del caso.

Ello supondría vaciar de contenido el necesario cumplimiento del principio de proporcionalidad en el acceso a los datos por las fuerzas y cuerpos de seguridad, derivado de los artículos 4.1 y 22.2 de la Ley Orgánica 15/1999, a los que se está haciendo continua cita en este lugar del informe.

De este modo, **debería incluirse en el precepto, siempre que sean tenidas en cuenta las observaciones que se han incluido en el presente apartado de este informe, la necesaria ponderación de la concurrencia de los requisitos citados con anterioridad y derivados esencialmente del artículo 22.2 de la Ley Orgánica 15/1999 para que pueda apreciarse la buena fe de la empresa de seguridad privada cedente de los datos**.

VI

Como se ha indicado, el segundo de los supuestos de acceso a la información de las empresas de seguridad se deriva del ejercicio de las competencias de inspección y control establecidas en el propio Anteproyecto

En este sentido, el artículo 12.1 del Anteproyecto establece que "corresponde a la Administración General del Estado, a través del Ministerio del Interior y, en su caso, de las Delegaciones y Subdelegaciones del Gobierno, el ejercicio de las competencias necesarias para el cumplimiento de lo dispuesto en esta ley, y específicamente" las correspondientes a "La autorización, inspección y sanción de las empresas de seguridad privada cuya competencia no haya sido asumida por las comunidades autónomas, así como cuando cuenten entre sus actividades de seguridad con la de protección personal o la de investigación privada" (letra a) y "la autorización, inspección y sanción de los despachos de detectives privados" (letra b).

En este ámbito, el artículo 52 regula las actuaciones de control disponiendo que "corresponde a las Fuerzas y Cuerpos de Seguridad competentes el cumplimiento de las órdenes e instrucciones que se impartan por los órganos a los que se refieren los artículos 12 y 13, en el ejercicio de las funciones de control de las empresas, servicios o actuaciones y del personal y medios en materia de seguridad privada".

A tal efecto, conforme al artículo 52.2 "en el ejercicio de estas funciones, los miembros de las Fuerzas y Cuerpos de Seguridad competentes podrán requerir la información pertinente y adoptar las medidas provisionales que resulten necesarias, en los términos del artículo 54". Además, los apartados 3 y 4 dispone que:

> *"3. Cuando en el ejercicio de las actuaciones de control se detectase la posible comisión de una infracción administrativa, se instará a la autoridad competente para la incoación del correspondiente procedimiento sancionador. Si se tratara de la posible comisión de un hecho delictivo, se pondrá inmediatamente en conocimiento de la autoridad judicial.*
>
> *4. Toda persona que tuviera conocimiento de irregularidades cometidas en el ámbito de la seguridad privada podrá denunciar aquéllas ante las autoridades o funcionarios competentes, a efectos del posible ejercicio de las actuaciones de control y sanción correspondientes."*

A su vez, el artículo 53.2 del Anteproyecto dispone que "2. Asimismo, al margen de los citados planes de inspección, cuando recibieren denuncias

sobre irregularidades cometidas por las personas físicas o jurídicas mencionadas en el apartado anterior o por los usuarios de esos servicios, procederán a la comprobación de los hechos denunciados y, en su caso, a instar la incoación del correspondiente procedimiento sancionador", añadiendo el artículo 53.3 que "a los efectos anteriormente indicados, las empresas y el personal de seguridad privada, así como los establecimientos obligados a contratar servicios de seguridad privada, los centros de formación y los usuarios que contraten dichos servicios, habrán de facilitar a las Fuerzas y Cuerpos de Seguridad competentes el acceso a sus instalaciones y medios a efectos de inspección, así como a la información contenida en los contratos de seguridad, en los expedientes de investigación y en los Libros-registros, en los supuestos y en la forma que reglamentariamente se determine".

Las normas citadas prevén el acceso por parte de las fuerzas y cuerpos de seguridad en el ejercicio de sus funciones de inspección, expresamente previstas en el Anteproyecto, a los datos que tuviera en su poder el sujeto sometido a la Ley, incluyendo los libros registros que el mismo ha de mantener. En particular, el artículo 49.4, en relación con los despachos de detectives privados añade, respecto del informe que preceptivamente deberán elaborar dichos despachos, y al que luego se hará referencia, que "dicho informe estará a disposición del cliente, entregándoselo a la finalización del servicio, así como de las autoridades policiales competentes para la inspección".

El acceso por el órgano que tenga atribuida por Ley la competencia para el desarrollo de las funciones de inspección y control de un determinado sector de actividad a los datos necesarios para el ejercicio de sus competencias debe, lógicamente, considerarse adecuado al contenido esencial del derecho fundamental a la protección de datos de carácter personal siempre que el mismo resulte congruente con los principios que delimitan ese contenido.

En particular debe nuevamente estarse al principio de proporcionalidad, tan citado a lo largo del presente informe, así como al de limitación de la finalidad, establecido en el artículo 4.2 de la Ley Orgánica 15/1999, a cuyo tenor "Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos".

De este modo, **sería conveniente que se especificase en el Anteproyecto que el tratamiento de los datos a los que se está haciendo referencia en este lugar sólo podrá llevarse a cabo para estas finalidades de inspección, no pudiendo los datos ser empleados por las fuerzas y cuerpos de seguridad para fines distintos y se limitará a los datos necesarios para la realización de tales funciones, no accediéndose a datos de carácter personal si ello no resultase necesario para el cumplimiento de los fines de inspección previstos en el Anteproyecto**.

Debe a estos efectos tenerse en cuenta que la citada recogida de datos implicará el tratamiento de los mismos por las fuerzas y cuerpos de seguridad dentro de los denominados ficheros administrativos a los que se refiere el artículo 22.1 de la Ley Orgánica 15/1999 cuando dispone que "Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley". Es decir, se está haciendo referencia a tratamientos totalmente diferenciados de los derivados de la investigación criminal y policial y que deben ser objeto de tratamiento separado y diferenciado, sin que quepa establecer ningún criterio de permeabilidad entre ambos tipos de ficheros, sin perjuicio de la licitud de las cesiones para la incorporación de los datos tanto a ficheros administrativos como policiales que se ha venido describiendo en los dos últimos apartados del presente informe.

VII

Dentro de los servicios de seguridad regulados por el Anteproyecto sometido a informe ya se indicó con anterioridad que resultan especialmente relevantes en relación con las materias objeto de competencia de esta Agencia los relativos a la videovigillancia y la actividad de los investigadores privados.

En relación con los primeros, excluida la aplicación de la Ley Orgánica 4/1997 de 4 agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y el ejercicio por esta Agencia de las competencias que pudieran derivarse de la misma, y como es sabido, la Agencia Española de Protección de Datos ha prestado especial atención a las cuestiones relacionadas con la videovigilancia, habiendo adoptado la Instrucción 1/2006, de 8 de noviembre, relacionada con el tratamiento de datos realizado a través de estos dispositivos de seguridad. Del mismo modo, han sido muy numerosas las resoluciones dictadas por esta Agencia en la materia, existiendo ya una doctrina judicial sobre la misma, emanada de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, que parte, como punto de partida del sometimiento de estos tratamientos a la normativa de protección de datos, al ser indiscutible la consideración de la imagen como dato de carácter personal, conclusión también alcanzada por la Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero, cuyo fundamento jurídico 5 señala que "Está fuera de toda duda que las imágenes grabadas en un soporte físico, como ha ocurrido en el caso de autos, constituyen un dato de carácter personal que queda integrado en la cobertura del art. 18.4 CE, ya que el derecho fundamental amplía la garantía constitucional a todos aquellos datos que identifiquen o permitan la identificación de la persona y que puedan servir para la confección de su perfil (ideológico, racial, sexual, económico o de cualquier otra índole) o para cualquier otra utilidad que, en determinadas circunstancias, constituya una amenaza para el individuo (STC 292/2000, de 30 de noviembre, FJ 6), lo cual,

como es evidente, incluye también aquellos que facilitan la identidad de una persona física por medios que, a través de imágenes, permitan su representación física e identificación visual u ofrezcan una información gráfica o fotográfica sobre su identidad".

El artículo 42 del Anteproyecto regula los servicios de videovigilancia, disponiendo lo siguiente:

> *"1. Los servicios de videovigilancia, a cargo de vigilantes de seguridad o, en su caso, de guardas rurales, consisten en la vigilancia de seguridad, a través de un sistema de videocámaras, fijas o móviles, con la exclusiva finalidad de protección de personas o bienes.*
>
> *2. La utilización de videocámaras estará presidida por los principios de proporcionalidad, idoneidad e intervención mínima.*
>
> *3. No se podrán utilizar videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en la legislación en materia de seguridad ciudadana, previa autorización administrativa. Su utilización en el interior de las viviendas requerirá el consentimiento del titular.*
>
> *4. Las cámaras de videovigilancia que formen parte de medidas de seguridad obligatorias o de sistemas de verificación de alarmas no requerirán autorización administrativa para su empleo o utilización.*
>
> *5. La grabación, tratamiento y registro de imágenes por parte de los sistemas de videovigilancia estará sometida a la normativa en materia de protección de datos de carácter personal."*

A nuestro juicio son tres las cuestiones principales a tomar en consideración en relación con este precepto: la primera, a la que ya se ha hecho referencia en un lugar anterior de este informe, se refiere a la delimitación de los supuestos legales habilitantes del tratamiento de los datos de las imágenes de las personas a través de los servicios de videovigilancia, teniendo particularmente en cuenta las exclusiones establecidas en los artículos 6 y 7 del Anteproyecto.

La segunda cuestión se refiere a los principios rectores del tratamiento de imágenes a través de los sistemas de videovigilancia, a los que se refieren los apartados 2 y 4 del artículo 42. Por último, y relacionada con dichos principios, deberán tenerse en cuenta los criterios establecidos en los apartados 3 y 4 de la norma objeto de informe, que afectan en gran medida a la proporcionalidad en el tratamiento y la posibilidad de grabación por los sistemas de videovigilancia de espacios públicos o de acceso público.

En cuanto a la primera de las cuestiones citadas, ya se hizo referencia en un lugar anterior de este informe a la evolución normativa en relación con la prestación de estos servicios y la causa legitimadora del tratamiento de los datos, fundándose ahora, siempre que la finalidad sea la garantía de la seguridad en los recintos privados en la concurrencia de un interés legítimo prevalente del responsable del fichero, al amparo de lo dispuesto en el artículo 7 f) de la Directiva 95/46/CE.

No obstante, conforme a lo ya señalado, del Anteproyecto no se desprende con claridad si las actividades que impliquen el tratamiento de imágenes a través de sistemas de videovigilancia exigirá o no que la empresa que proceda al tratamiento reúna determinados requisitos y, en particular, que cuando el establecimiento de estos sistemas se lleve a cabo como medida de autoprotección, de las previstas en el artículo 7 del Anteproyecto sea posible el uso de videocámaras sin contar para ello con una empresa de seguridad privada.

Este problema puede incluso acrecentarse con lo dispuesto en el artículo 42.1 del Anteproyecto, ya que de su tenor no puede deducirse claramente si los servicios regulados por el precepto serán únicamente los incluidos en el ámbito de aplicación de la norma o si dichos servicios se refiere a cualquier supuesto de instalación de dispositivos de videovigilancia por el titular de las instalaciones objeto de esta medida de seguridad.

Como también se ha indicado con anterioridad, el criterio de esta Agencia ha sido el de considerar que la normativa de seguridad privada resulta de aplicación en los supuestos de conexión del dispositivo a una central de alarmas, de suerte que en caso contrario, es decir cuando la visualización se lleva a cabo por el propio titular o la persona a la que el mismo se encomiende el visionado y no exista tal conexión, no sería precisa la concurrencia de un prestador de servicios de seguridad privada.

Al propio tiempo, es preciso tener en cuenta que el artículo 46.1 del Anteproyecto dispone que “Los servicios de instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, consistirán en la ejecución, por técnicos acreditados, de todas aquellas operaciones de instalación y mantenimiento de dichos aparatos, equipos, dispositivos o sistemas, que resulten necesarias para su correcto funcionamiento y el buen cumplimiento de su finalidad, previa elaboración, por parte de ingenieros acreditados, del preceptivo proyecto de instalación, cuyas características se determinarán reglamentariamente”, añadiendo el artículo 46.2 que “estos sistemas deberán someterse a revisiones preventivas con la periodicidad y forma que se determine reglamentariamente”, pudiendo derivarse de lo dispuesto en este precepto que la instalación y mantenimiento debería ser llevada a cabo por las entidades y profesionales debidamente acreditados, a los que quedaría restringido el ejercicio de esta actividad.

De este modo, esta Agencia debe insistir en la necesidad de que **el Proyecto sea más terminante en la delimitación de su ámbito de aplicación en relación con el servicio de seguridad al que se está haciendo referencia, pudiendo a tal efecto, si se considera que la autoprotección y la consiguiente instalación y mantenimiento de los dispositivos se encuentran excluidos del ámbito de la norma, hacer constar en el artículo que lo dispuesto en el mismo se aplicará a los supuestos en los que los servicios se lleven a cabo por empresas de seguridad privada o con conexión a una central de alarmas o como complementarios de otros servicios de seguridad privada y excluyendo expresamente en el precepto la autoprotección a la que se refiere el artículo 7. Del mismo modo, el artículo 46 debería complementarse haciendo referencia, en caso de alcanzarse la conclusión a la que aquí se está haciendo mención, al ámbito derivado del artículo 42 en caso de que el mismo se complete en los términos propuestos**.

VIII

La segunda de las cuestiones a la que se ha hecho referencia se deriva da la aplicación de los principios que, a tenor de lo dispuesto en el Anteproyecto, deben gobernar la utilización de los dispositivos de videovigilancia, diferenciando en el apartado 2 los principios de proporcionalidad, idoneidad e intervención mínima de la aplicación según el artículo 5 de la normativa de protección de datos de carácter personal a la grabación, tratamiento y registro de las imágenes.

Como punto de partida, debe indicarse que la aplicación los principios señalados en el artículo 42.2 deriva directamente de la aplicación de las normas de protección de datos, y especialmente del principio de proporcionalidad, que tantas veces se ha mencionado a lo largo de este informe. Así lo recordaba la Exposición de motivos de la Instrucción 1/2006 de esta Agencia, teniendo en cuenta la doctrina del Tribunal Constitucional, cuando señalaba lo siguiente:

> *"En cuanto a la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad».*

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

Asimismo la proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, tales como la instalación de sistemas de vigilancia en espacios comunes, o aseos del lugar de trabajo. Por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona."

De este modo, debe entenderse que la aplicación de los principios citados en el artículo 42.2 del Anteproyecto sometido a informe no es más que una consecuencia directa de la aplicación de las normas de protección de datos, toda vez que es el visionado o la grabación de las imágenes la que supone una restricción de los derechos fundamentales de los visionados o grabados.

Por otra parte, la referencia realizada en el artículo 42.5 a la "grabación, tratamiento y registro" podría introducir cierta confusión en lo referente al alcance de la aplicación de la normativa de protección de datos al tratamiento de los datos de las imágenes. En este sentido, debe recordarse que el párrafo segundo del artículo 1.1 de la Instrucción 1/2006 establece que "El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas", entendiendo que todas estas actividades encajan dentro de la definición de tratamiento de datos establecida por el artículo 3 c) de la Ley Orgánica 15/1999.

Teniendo en cuenta todo lo anterior, **esta Agencia considera que sería conveniente fusionar en un solo apartado lo previsto en los apartados 2 y 5 del artículo 42 del Anteproyecto, estableciendo que el tratamiento de las imágenes recogidas a través de sistemas de videovigilancia, tanto si las mismas son objeto de grabación como si únicamente son reproducidas o emitidas en tiempo real se encontrará sometido a la normativa de protección de datos de carácter personal, añadiendo que en la utilización**

de estos dispositivos se respetarán los principios de proporcionalidad, idoneidad e injerencia mínima.

IX

Por último, como se señaló, la tercera cuestión a tomar en consideración en relación con lo dispuesto en el artículo 42 del Anteproyecto guarda relación con los límites de la posible utilización de sistemas de videovigilancia y la posible autorización de los mismos en supuestos excepcionales.

En relación con este punto, debe tenerse particularmente en consideración lo dispuesto en el artículo 4.3 de la Instrucción 1/2006, en que se señala que "las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida".

Por otra parte, se ha venido planteando el problema de la delimitación de los supuestos en los que es o no posible la instalación de dispositivos de videovigilancia. Dados los distintos conceptos empleados para delimitar los ámbitos de actuación, por cuanto mientras la Ley Orgánica 4/1997, que establece un límite de exclusión al uso de estos dispositivos como medida de seguridad privada hace referencia a "vías y espacios públicos", otras normas se refieren, como el proyecto, para delimitar el campo de exclusión a "vías y espacios públicos o de acceso público", siendo parcialmente similar la solución ofrecida por la citada Instrucción 1/2006.

La Agencia española de Protección de Datos ha analizado cuándo cabe apreciar que se da la proporcionalidad establecida en la mencionada Instrucción 1/2006 especialmente en su resolución de 20 de diciembre de 2012, ya citada en un lugar anterior, cuyo contenido, pese a su extensión debe reproducirse parcialmente en este lugar:

> *"Sentado todo ello, la aplicación de las causas de legitimación analizadas en el punto anterior a los supuestos de captación de imágenes a través de sistemas de videovigilancia implica la posible concurrencia de dos supuestos diferenciados:*
>
> *Un primer caso será el de instalación de los citados dispositivos en los denominados "espacios públicos" a los que se refiere la Ley Orgánica 4/1997. En estos supuestos, el tratamiento de los datos será legítimo, por encontrarse amparado en una norma con rango de Ley (artículo 6.1 de la LOPD), siempre y cuando se cumplan los requisitos exigidos por la*

citada Ley Orgánica para que la instalación pueda tener lugar y únicamente cuando se cumplan efectivamente tales exigencias.

En los restantes supuestos, y siempre que no sea de aplicación la excepción doméstica contenida en el artículo 2.2 a) de la LOPD, la legitimación para el tratamiento de imágenes con fines de videovigilancia para preservar la seguridad de las instalaciones únicamente podrá venir fundada en lo dispuesto en el artículo 7 f) de la Directiva 95/46/CE, al no ser posible recabar el consentimiento de las personas cuyas imágenes sean objeto de captación, ni existir una norma con rango de Ley que habilite el tratamiento ni ser aplicables las excepciones establecidas en el artículo 6.2 de la LOPD.

Como se ha indicado reiteradamente, el problema en la delimitación de uno y otro supuesto es que el concepto utilizado por el legislador ha sido el de "espacios públicos" y "lugares públicos", respecto del que no existe un concepto legal, por lo que será preciso analizar cuando cabrá considerar que nos encontramos ante uno u otro supuesto. Para ello deberá tenerse en cuenta la doctrina emanada de la Audiencia Nacional, a fin de conocer respecto de qué zonas podría eliminarse la incertidumbre que pudiera generar la utilización por las normas que hemos venido citando de un concepto jurídico indeterminado.

Un primer criterio que permitirá delimitar los supuestos en los que diferirá la legitimación para el tratamiento ha sido el de equiparar "espacios públicos" y "lugares públicos" con "vía pública".

En este sentido, la Sentencia de la Audiencia Nacional de 10 de febrero de 2012 señala lo siguiente:

"Las cámaras instaladas en el perímetro del edificio y que constan ubicadas en los planos del mismo (...) permiten captar imágenes no sólo de las fachadas que se encuentran en la vía pública, sino de la propia vía pública más allá de lo que en este caso se considera idóneo y proporcional al fin perseguido. Téngase en cuenta que se trata de cámaras domo "móviles", por lo que su ámbito de visión puede desplazarse 360º y grabar a las personas que transitan por la vía pública, no circunscribiéndose por tanto, como alega la recurrente, a controlar los accesos al edificio. (...)

La grabación de imágenes en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad del Estado, de acuerdo con lo establecido en la Ley Orgánica 4/1997 y no se ha acreditado que la recurrente tuviera autorización administrativa al respecto.

Por tanto, al haberse efectuado la captación y grabación de imágenes de personas identificables en la vía pública (datos de carácter personal ex

artículo 3.a) LOPD), más allá de lo que, como se ha dicho, se considera idóneo y proporcional al fin perseguido, criterios de proporcionalidad a los que se refiere la citada Instrucción 1/2006, se ha producido un tratamiento de datos de carácter personal, atendidos los amplios términos del concepto de tratamiento de datos de carácter personal contenido en el artículo 3.c) de la LOPD. Tratamiento de datos para el que la Diputación recurrente no está legitimada al tener lugar la captación de imágenes en la vía pública, por lo que al haberse efectuado sin contar con el consentimiento de las personas afectadas, dicha conducta de la Diputación Provincial de Málaga integra la infracción tipificada en el artículo 44.3.d) en relación con el artículo 6 ambos de la LOPD, apreciada por la resolución recurrida."

De lo indicado en esta sentencia cabe inferir que a juicio de la Audiencia Nacional no existe duda de que la grabación de imágenes en la vía pública fuera de las reglas de proporcionalidad exigidas por el artículo 4.3 de la Instrucción 1/2006 implicará la captación de imágenes en espacios públicos respecto de la que la única posible causa legitimadora del tratamiento será la habilitación conferida por la Ley Orgánica 4/1997. Es decir, como primer criterio de delimitación habrá que entender que dentro del concepto de "espacio público" se encontrará la "vía pública", no alcanzando a la grabación de la misma, con carácter general, la legitimación que pudiera derivarse de la aplicación de la regla de ponderación establecida en el artículo 7 f) de la Directiva 95/46/CE.

Ahora bien, la conclusión alcanzada no implica automáticamente que la instalación de dispositivos de videovigilancia siempre sea posible cuando las imágenes no capten la "vía pública" o la captación se limite a la mínima imprescindible establecida en el artículo 4.3 de la Instrucción 1/2006 de esta Agencia.

A tal efecto, conviene traer a colación lo señalado por la Sentencia de la Audiencia Nacional de 20 de mayo de 2011, ya citada en la resolución recurrida:

"(..) el hecho de que dicho sistema de videovigilancia haya sido instalado conforme a la normativa de seguridad, no autoriza a la Asociación recurrente a realizar grabaciones de imágenes en la vía pública más allá de lo que resulta idóneo, adecuado y proporcional, siendo igualmente indiferente, a estos efectos, que la instalación material de tales cámaras se encuentre o no dentro de la propiedad privada pues lo esencial es el carácter privado o público de las imágenes captadas y grabadas, es decir, si tales imágenes afectan o no a personas que se encuentran en lugares públicos, en cuyo caso tal tratamiento ha de respetar el principio de proporcionalidad."

Debe recalcarse que si bien dicha sentencia se refiere en principio a la captación de la vía pública, respecto de la que niega la posible existencia de legitimación para el tratamiento derivada de la instalación de la videocámara, hace posteriormente referencia al concepto de "espacios públicos", en los que se encuentra necesariamente la vía pública, pero sin establecer una identidad absoluta entre unos y otros.

(…)

Y es aquí donde deberá tenerse particularmente en cuenta la regla de ponderación exigida por el artículo 7 f) de la Directiva 95/46/CE para que pueda entenderse que un tratamiento se encuentra debidamente legitimado. Como se ha dicho, para que ello sea posible será preciso apreciar no sólo la concurrencia de un interés legítimo en el responsable del tratamiento, sino que además la intromisión que el tratamiento produce en los derechos de los interesados resulte proporcional, de forma que en caso de que la finalidad perseguida por el tratamiento puede alcanzarse a través de medidas menos lesivas para dicho derecho fundamental que la consistente en el tratamiento de sus datos sean aquéllas y no el tratamiento la medida adoptada en definitiva.

En consecuencia, dado que las normas aplicables a la instalación de dispositivos de videovigilancia se refiere a los términos "espacios públicos" y "lugares públicos" y no a los de "vía pública" o "dominio público" a la hora de delimitar las causas legitimadoras del tratamiento, será preciso que cuando las grabaciones se lleven a cabo en lugares de acceso o uso público que no tengan la consideración de "vía pública" o "dominio público" se lleve a cabo la ponderación de los legítimos intereses que pudieran fundamentar la instalación del dispositivo por parte del propietario o titular del uso de los lugares objeto de vigilancia y los derechos de los interesados que serán grabados mediante la instalación de los dispositivos. Sólo cuando quepa considerar que la medida adoptada es coherente con la ponderación exigida por el artículo 7 f) de la Directiva será igualmente posible considerar que en los supuestos no contemplados en la Ley Orgánica 4/1997 la instalación de dispositivos de videovigilancia y el consiguiente tratamiento de datos derivado de la misma se encuentran legitimados por la legislación de protección de datos.

En este sentido, esta Agencia ya ha venido efectuando la ponderación a la que se está haciendo referencia en distintas resoluciones, como la recaída en el procedimiento PS/00551/2011, referido a la captación de imágenes en una estación de servicio, en la que se señala (letra c) del fundamento de derecho VI) lo siguiente:

"se ha observado en el presente procedimiento que las imágenes que captan la cámara denunciada no son desproporcionadas para la

finalidad que tienen de control de la estación de servicio, ajustándose a lo previsto en la Instrucción 1/2006 de videovigilancia en su artículo 4.3 que señala que "Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida."."

Y en este punto cobran relevancia las específicas circunstancias que concurren en el presente supuesto, dado que las videocámaras recogen imágenes de zonas que, aun siendo libremente accesibles por los interesados, lo que podría calificarlas como "espacios públicos", se encuentran incorporadas al patrimonio de ADIF; es decir, dichos inmuebles son de propiedad privada. Además, como se ha indicado la instalación de las videocámaras trae su causa de lo establecido en el Convenio celebrado entre ADIF y RENFE-Operadora, "suscrito, previa tramitación reglamentaria" y publicado en el Boletín Oficial del Estado como consecuencia de la correspondiente Resolución de la Secretaría General de Infraestructuras, en el que se impone expresamente a RENFE-Operadora la obligación de velar por la seguridad de las instalaciones a las que el mismo se refiere, entre las que se encuentran expresamente las tres estaciones objeto del presente procedimiento y, particularmente, los aparcamientos de las mismas. Además, tal y como se ha indicado, se han cumplido las previsiones de la Instrucción 1/2006 en lo relativo al cumplimiento al deber de información y la creación y notificación del correspondiente fichero, habiéndose finalmente adoptado cautelas para garantizar que el acceso a las imágenes quede limitado a las personas concretas a las que el responsable del fichero encomienda las funciones de seguridad.

Teniendo en cuenta tales antecedentes, y en tanto la grabación de las imágenes se limite a los recintos a los que se refiere el Convenio, entre los que se encontrarían las estaciones y las instalaciones vinculadas a las mismas, como son en este caso los aparcamientos, y siempre y cuando no se exceda la regla de proporcionalidad a la que se refiere el artículo 4.3 de la Instrucción 1/2006 en cuanto a los espacios no privados que excedan del alcance del mencionado Convenio, cabrá considerar que el tratamiento de los datos se encuentra amparado por lo dispuesto en el artículo 7 f) de la Directiva 95/46/CE, dotado de efecto directo en nuestro derecho, tal y como prescribe la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011."

Al propio tiempo, y en cuanto a la posibilidad de utilización de sistemas de videovigilancia en supuestos excepcionales aun cuando el uso de los mismos implique la captación (de modo accesorio) de la vía pública o de espacios públicos, esta Agencia ha tenido la ocasión de pronunciarse en

informe de 17 de mayo de 2011, emitido en relación con la posibilidad de que por parte de un operador de telecomunicaciones se instalasen videocámaras dirigidas a los espacios en que se encontraban arquetas de registro cuyo carácter estratégico había sido declarado por la Comisión del Mercado de las Telecomunicaciones. En el citado informe se concluía que "a la vista de todo lo que se ha venido indicando cabe concluir que la instalación de las videocámaras a las que se refiere la consulta resulta conforme a lo dispuesto en la Ley Orgánica 15/1999 y su normativa de desarrollo siempre que se dé cumplimiento a los criterios de proporcionalidad referidos en el apartado X de este informe, se refuerce el deber de información a los interesados en los términos indicados en el apartado XI y se notifique la creación de un fichero separado y relacionado únicamente con estos tratamientos, como se indica en el apartado XII", añadiendo que "en todo caso, la consultante deberá comunicar a esta Agencia cualquier nuevo supuesto en el que pretendan llevarse a cabo actividades de videovigilancia de las arquetas de registro y que no aparezca recogido en la enumeración adjunta a la consulta.

En cuanto a los citados criterios de proporcionalidad, se señalaba en el informe lo siguiente:

> *"Teniendo en cuenta la variedad de supuestos a la que acaba de hacerse referencia no resulta posible efectuar un juicio individualizado de la concurrencia en cada supuesto concreto del principio de proporcionalidad en los términos que se han descrito, si bien a la vista de la información aportada es posible delimitar los criterios que permitirían determinar si se da o no la mencionada proporcionalidad.*
>
> *a) Así, un primer criterio sería el de proximidad de la cámara respecto de la arqueta objeto de la videovigilancia. Siguiendo este criterio, la proporcionalidad se cumpliría en mayor medida cuanto más próxima se encuentre la cámara a la arqueta, de forma que la imagen relacionada con la misma y que permita captar las situaciones de manipulación o sabotaje sea más nítida como consecuencia de dicha proporcionalidad. A título de ejemplo, la instalación de una videocámara que permita obtener una imagen cenital de la arqueta de forma que sea dicha imagen la que ocupe una mayor superficie de la visualizada o grabada cumpliría en mayor medida el principio de proporcionalidad que la imagen tomada desde una cámara situada a una distancia considerable de la arqueta y que permite únicamente una apreciación difusa de la misma y de la manipulación que de aquélla pudiera realizarse.*
>
> *Lógicamente, el criterio que acaba de indicarse quedará limitado por la propia fachada del edificio, al no ser posible la instalación de una videocámara más allá de los límites de la instalación usada por la consultante, lo que permite concluir que la cámara debería ser instalada en la zona de la fachada del edificio de la consultante que resulte más próxima a la arqueta de registro cuya videovigilancia se pretende.*

b) El segundo criterio a tener en cuenta para determinar si se da o no la proporcionalidad exigida por la Ley será el derivado del propio ángulo de visión de la cámara que lleve a cabo la videovigilancia de la arqueta de registro. Según este criterio, la imagen cubierta por la grabación no debería extenderse a una zona de la vía pública que resulte alejada de la arqueta en una distancia mayor a la necesaria para garantizar la seguridad y poder captar las posibles manipulaciones o sabotajes que se pretenden evitar.

De este modo, por ejemplo, en caso de que la arqueta apareciese en el centro de la imagen, permitiendo a su alrededor la grabación de un radio superior al necesario para tal fin (por ejemplo, toda la acera de la vía en caso de ser amplia o la calzada en caso de que quien pretendiera manipular la arqueta debiera introducirse en la acera para lograr tal fin) excedería el principio de proporcionalidad. Por el contrario, nuevamente, si la imagen obtenida se limita a la arqueta y un mínimo radio a partir de la misma se estaría dando cumplimiento al principio de proporcionalidad.

Por este mismo motivo, en caso de que la arqueta no se encontrase en el margen de la fachada del edificio, la imagen captada debería situar la arqueta en el extremo de la misma, a fin de no proceder a la visualización o grabación de imágenes innecesarias que pudieran vulnerar el citado principio de proporcionalidad.

c) En tercer lugar, y siguiendo la doctrina sentada en la Sentencia de la Audiencia Nacional de 11 de marzo de 2011, reproducida en un lugar anterior de este informe, sería preciso que la grabación evitase en todo lo que fuera posible la captura de imágenes de las vías públicas y calzadas y, siempre que ello fuera posible, de datos tales como las matrículas de los vehículos situados en los alrededores de la arqueta objeto de la vigilancia.

d) Por último, y recogiendo igualmente el criterio sustentado en esa sentencia, las instalaciones deberían ser fijas, al deber dirigirse la vigilancia a la propia arqueta, no produciéndose así grabaciones de trescientos sesenta grados, respecto de las que la Sentencia de 10 de febrero de 2011 vino a declarar la desproporcionalidad en el tratamiento."

De todo lo antedicho se desprenden ciertas consecuencias que pudieran afectar a la aplicación concurrente de las normas de protección de datos y las contenidas en el Anteproyecto sometido a informe:

En primer lugar, la referencia efectuada por el apartado 3 a las "vías y espacios públicos o de acceso público" como supuestos excluidos completamente de la videovigilancia, salvo que así lo prevea la legislación de

seguridad ciudadana y, en todo caso, sometiendo dicha posibilidad a un régimen de autorización puede resultar excesiva, toda vez que, conforme se desprende de la Instrucción 1/2006 y de la propia realidad en la mayor parte de los supuestos resulta imposible la instalación de estos dispositivos sin que los mismos puedan cubrir una parte, aun cuando haya de ser mínima, de la vía pública (por ejemplo, el área de entrada a un determinado recinto), también es posible que existan zonas de libre acceso, como la del supuesto analizado en la resolución de 20 de diciembre de 2012, ya citada, en que el establecimiento de estos sistemas constituya una medida proporcional e idónea de vigilancia, incluso aunque el acceso a las áreas vigiladas no se encuentre restringido al tráfico (por ejemplo, mediante el establecimiento de una barrera física de entrada), siempre que concurran los criterios de proporcionalidad y ponderación que se han analizado.

Por último, en cuanto al establecimiento del régimen de autorización el mismo puede resultar una solución en supuestos específicos en que el objeto directo de la vigilancia sea la vía pública, aun cuando dicha vigilancia tenga por finalidad esencial la seguridad de efectos de naturaleza privada, como sucede en el caso analizado en el informe de 17 de mayo de 2011 que también se ha citado, teniendo en cuenta que en dicho supuesto no se había considerado necesaria la emisión de autorización alguna. No obstante, sería conveniente restringir el número de supuestos en los que la autorización a fin de hacer viable la aplicación de la norma.

Por todo ello, esta Agencia considera que debería matizarse el tenor de lo dispuesto en el apartado 3 del artículo 42 del Anteproyecto a fin de, en primer lugar, no establecer una exclusión absoluta (salvo autorización) de la captación de imágenes de vías o espacios públicos y, en segundo término especificar con mayor detalle los supuestos en los que será precisa la autorización administrativa. Así, se propone la siguiente redacción

> ***"3. Sólo se podrán utilizar videocámaras con fines de seguridad privada que capten imágenes de vías públicas en la medida en que resulten necesarias para la seguridad de los espacios privados objeto de la vigilancia o, tratándose de espacios públicos o de acceso público cuando analizadas las circunstancias de su instalación y ponderados los derechos de las personas cuyas imágenes puedan ser captadas por medio de las cámaras, quepa considerar prevalente la garantía de la seguridad de las personas y bienes en dichos espacios.***
>
> ***Fuera de los supuestos señalados en el párrafo anterior, la utilización de videocámaras en vías o espacios públicos o de acceso público sólo será posible en los supuestos y en los términos y condiciones previstos en la legislación en materia de seguridad ciudadana, previa autorización administrativa.***

La utilización en el interior de las viviendas requerirá el consentimiento del titular.

Se prohíbe en todo caso la captación de sonidos en las vías y espacios públicos o de acceso público."

X

En relación con los servicios de investigación privada, debe partirse del artículo 37.1 del Anteproyecto, según el cual "Los detectives privados, a solicitud de personas físicas o jurídicas, se encargarán del ejercicio de las siguientes funciones: a) Obtener y aportar información y pruebas sobre conductas o hechos privados por encargo de los que tengan un interés legítimo en el asunto. b) Investigar delitos perseguibles sólo a instancia de parte por encargo de los legitimados en el proceso penal".

En este contexto, el artículo 49.1 del texto sometido a informe dispone que "Los servicios de investigación privada, a cargo de detectives privados, consistirán en la obtención y aportación de información y pruebas sobre conductas o hechos privados que afecten al ámbito económico, laboral, mercantil, financiero y, en general, a la vida personal, familiar o social, exceptuada la que se desarrolle en los domicilios o lugares reservados, así como en la realización de las averiguaciones que resulten necesarias en relación con la investigación de delitos sólo perseguibles a instancia de parte por encargo de los legitimados en el proceso penal, o para garantizar el normal desarrollo de determinados eventos".

Esta Agencia ha venido considerando lícito el tratamiento de datos de carácter personal que pueda derivarse de la realización de actividades de investigación privada, siempre que resulte ajustado a los principios de proporcionalidad y finalidad y siempre que quede circunscrita al ámbito del encargado en cuyo seno se desarrolla la actividad investigadora, que deberá igualmente respetar los citados principios. En este sentido se pronuncia, aunque de forma indirecta la sentencia de la Audiencia nacional de 20 de mayo de 2010, cuando afirma lo siguiente:

"Argumenta también (la recurrente) *que viene actualizando los datos de los particulares contenidos en sus bases de datos mediante una mercantil dedicada a la seguridad privada y ningún detective privado tiene obligación de desvelar sus fuentes de información amparándose en el secreto profesional que asiste a su labor profesional. Argumentación que <u>podría justificar, en su caso, la exención de la necesidad de consentimiento para la inclusión de los datos personales en los ficheros de tal empresa de detectives</u>, pero no para la inclusión de los datos en los propios ficheros de la entidad sancionada, precisamente por*

tratamiento inconsentido de datos en sus ficheros, que es (la recurrente) *y no la empresa de detectives."*

En el mismo sentido, la sentencia de la Audiencia Nacional de 8 de mayo de 2012 afirma que "esta Sala comparte la argumentación de la resolución impugnada en el sentido de considerar improcedente iniciar procedimiento sancionador, por infracción de la Ley de Protección de Datos, como consecuencia de la incorporación al procedimiento judicial de una prueba de video, realizada en la vía pública, por una agencia de detectives privados, en la que además de la imagen de la persona frente a quien se dirige el procedimiento, aparezcan también las de determinados familiares del mismo".

No obstante, como cabe apreciar en el texto reproducido en primer lugar y se desprende del segundo, la normativa de seguridad privada actualmente en vigor no legitima cualquier tratamiento de datos por parte de los detectives privados, sino que dicho tratamiento queda limitado por dos principios especialmente relevantes: la existencia de un interés legítimo que justifique la realización de las tareas de investigación y la garantía de los derechos consagrados en el artículo 18 de la Constitución.

En este sentido, el artículo 49.2 del Anteproyecto incorpora el primer de los límites citados, al indicar que "La aceptación de estos servicios por parte de los detectives privados requerirá, en todo caso, la existencia de un interés legítimo por parte del cliente contratante del servicio debiendo ejecutarse el mismo con respeto a los criterios de razonabilidad, necesidad, idoneidad y proporcionalidad", debiendo considerarse acertada la inclusión de ese límite a la realización de las investigaciones privadas.

En cuanto al segundo de los límites, el artículo 49.3 dispone que "En ningún caso podrán utilizarse en este tipo de servicios medios materiales o técnicos de tal forma que atenten contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones".

Ciertamente la norma reproduce lo actualmente dispuesto en la Ley 23/1992. No obstante, no debe perderse de vista que en el momento en que la misma fue adoptada no existía aún un desarrollo de lo dispuesto en el artículo 18.4 de la Constitución, que tuvo lugar pocos meses después con la aprobación de la Ley Orgánica 5/1992, ni la doctrina del Tribunal Constitucional había configurado inequívocamente el derecho a la protección de datos de carácter personal como un derecho fundamental independiente y autónomo de los demás consagrados por el artículo 18 de la Carta Magna. De este modo, **sería conveniente que el Anteproyecto incluyera el derecho fundamental a la protección de datos dentro de los límites de la actuación de investigación privada contenidos en el artículo 49.3, dada la especial naturaleza de este derecho** y sin que sea un obstáculo para ello el hecho de que el apartado 5 haga referencia a la normativa de protección de datos al referirse a la conservación de imágenes y sonidos, por cuanto este derecho

debe gobernar la totalidad de la actividad de los investigadores privados, del mismo modo que la gobiernan los restantes derechos consagrados por el artículo 18 de la Constitución.

En cuanto a las especialidades relacionadas con los tratamientos de datos llevados a cabo por los investigadores privados, el artículo 49 establece dos reglas específicas: la emisión del informe al que se refiere el apartado 4 y la conservación de datos relacionada en el apartado 5. Además, las cesiones de datos se limitan según el artículo 49.6 al propio cliente y a los órganos judiciales y administrativos.

Respecto del informe, ya se ha señalado en un lugar anterior que la única cuestión que resulta susceptible de análisis en relación con el texto contenido en el Anteproyecto es la relativa al acceso a los datos contenidos en aquél por parte de las autoridades policiales competentes para la inspección, debiéndose tener en cuenta lo que ya se dijo en cuanto a la minimización de los datos respecto de los que se producirá el acceso, de modo que **el conocimiento del contenido íntegro de los informes debería restringirse a los supuestos mínimos imprescindibles, previniéndose asimismo la cautela de que los datos únicamente podrán ser tratados en el contexto de esa actuación inspectora y no utilizarse para otros fines**.

Por su parte, en relación con las cesiones de datos previstas en el artículo 49.6, aun considerándose ajustadas al contenido esencial del derecho fundamental a la protección de datos, sería necesario que se clarificase con mayor precisión cuáles serán las causas que justifiquen el acceso policial a los datos (la existencia de indicios de delito perseguible de oficio y, en su caso, la realización de actuaciones de inspección en el marco de la propia Ley). En particular **sería preciso que se especificasen los fines para los que se podrá proceder a la utilización de los datos por parte de los clientes, que deberían encaminarse únicamente a la persecución de los delitos perseguibles a instancia de parte, en caso de que ese sea el objeto de la investigación o a los fines legítimos a los que se refiere el artículo 49.2 del Anteproyecto**.

Finalmente, debe hacerse referencia a las reglas de conservación del artículo 49.5 del Anteproyecto, que dispone que “los informes a que se refiere el apartado anterior deberán conservarse archivados, al menos, durante cinco años”, añadiendo que “Las imágenes y los sonidos grabados durante las investigaciones o vigilancias se destruirán un año después de su finalización, salvo que estén relacionadas con un procedimiento judicial, una investigación policial o un expediente sancionador”. “En todo caso (concluye el texto), el tratamiento de dichas imágenes y sonidos deberá observar lo establecido en la normativa sobre protección de datos de carácter personal”.

En lo que respecta a los informes, debería justificarse la causa en cuya virtud el plazo de conservación será de cinco años, habida cuenta que el

informe únicamente podrá ser objeto de comunicación a los clientes, lo que sucederá al término de la investigación, o a las autoridades policiales competentes en materia de inspección, siendo así que el plazo de prescripción de las infracciones muy graves es de dos años, conforme al artículo 55.2 del texto sometido a informe. De este modo, a menos que el informe haya de incorporarse a unas diligencias judiciales o de investigación policial no sería preciso el establecimiento de un plazo de cancelación superior al citado de dos años.

En este sentido, debe recordarse que el artículo 4.5 de la Ley Orgánica 15/1999, que forma parte de su contenido esencial, dispone que "Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados", de forma que "No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados".

La cancelación de los datos, desde el punto de vista de la aplicación de las normas de protección de datos, no implica su borrado físico, sino que de conformidad con el artículo 16.3 de la Ley Orgánica 15/1999 "dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas". De este modo, dado que la comunicación del dato a las autoridades judiciales o policiales se encontraría dentro de este supuesto nada se opone a que **el plazo de conservación debiera ser el de dos años, sin perjuicio de su bloqueo posterior en los términos señalados**.

En cuanto a las imágenes y sonidos, **debería justificarse el motivo que justifica la conservación durante un período de un año, sobre todo teniendo en cuenta que respecto de las imágenes captadas a través de dispositivos de videovigilancia la normativa de protección de datos, a la que se remite como se ha visto el artículo 42 del Anteproyecto, establece un plazo de conservación de sólo un mes**, todo ello sin perjuicio del deber de bloqueo posterior a la cancelación, en su caso.

En este sentido, el inciso final del apartado al que se está ahora haciendo referencia sólo alcanzará la debida congruencia en caso de que se establezca la reducción de los plazos de conservación que se acaban de indicar, toda vez que, como se ha dicho, son las propias normas de protección de datos las que justifican que los plazos sean los citados, **aunque cabría indicar en el precepto que la conservación a la que el mismo se refiere se entiende sin perjuicio del bloqueo de los datos establecido en dicha normativa, en los términos que también se han descrito**.

XI

Resta por último hacer referencia al régimen sancionador contenido en el Anteproyecto sometido a informe, por cuanto el mismo contiene una serie de tipos sancionadores que colisionan con los establecidos en la Ley Orgánica 15/1999.

Así, el artículo 56 se refiere a las infracciones que podrán ser cometidas por las empresas de seguridad privada, incluyendo como infracciones muy graves "La realización de actividades prohibidas en el artículo 8.5, sobre reuniones o manifestaciones, conflictos políticos o laborales, control de opiniones o su expresión o creación o mantenimiento de ficheros, automatizados o no, de datos de carácter personal sobre las mismas, e información a terceras personas sobre clientes, personas relacionadas con éstos o con bienes de cuya seguridad estén encargados, o cualquier otra forma de quebrantamiento del deber de reserva, cuando no sean constitutivas de delito" (apartado 1 c), así como "La instalación o utilización de sistemas de videovigilancia, así como los correspondientes a la captación de imágenes o sonido por los sistemas de alarma, incumpliendo los requisitos o finalidades establecidos para ellos (apartado 1 j). Asimismo, será infracción grave "La conservación, fuera de los plazos y supuestos establecidos en cada caso, de las imágenes y sonidos grabados por los sistemas de videovigilancia, los sistemas de verificación de alarmas y las correspondientes a investigaciones privadas, conculcando el deber de destruirlos exigido por los artículos 42 y 49.5" (apartado 2 m).

Por su parte, el artículo 57 se refiere a las infracciones cometidas por el personal de seguridad, entre las que se encuentran, tipificadas como muy graves "La falta de reserva debida sobre las investigaciones que realicen los detectives privados o la utilización de medios materiales o técnicos de tal forma que atenten contra el derecho al honor, a la intimidad personal o familiar, a la propia imagen o al secreto de las comunicaciones" (apartado 1 c) y "La realización de actividades prohibidas en el artículo 8.5 sobre reuniones o manifestaciones, conflictos políticos y laborales, control de opiniones o su expresión o creación o mantenimiento de ficheros, automatizados o no, de datos de carácter personal, sobre las mismas, e información a terceras personas sobre clientes, personas relacionadas con éstos o bienes de cuya seguridad estén encargados, en el caso de que no sean constitutivas de delito" (apartado 1 g). Además, es infracción leve "La conservación, fuera de los plazos y supuestos establecidos, de las imágenes y sonidos grabados por los sistemas de videovigilancia, los sistemas de verificación de alarmas y las correspondientes a investigaciones privadas, conculcando el deber de destruirlos exigido por los artículos 42 y 49.5" (apartado 2 g).

Las conductas citadas con anterioridad implican asimismo la comisión de infracciones en materia de protección de datos de carácter personal. Así, el mantenimiento de bases de datos o ficheros con datos especialmente

protegidos, a la que se refiere la prohibición del artículo 8.5 del Anteproyecto supone un tratamiento sin consentimiento de los mencionados datos, tipificado como infracción muy grave de la Ley Orgánica por el artículo 44.4 b) de la Ley Orgánica 15/1999.

Por otra parte, la instalación de dispositivos de videovigilancia sin el cumplimiento de los requisitos legalmente establecidos debe considerarse como un supuesto de tratamiento sin consentimiento de datos de carácter personal, tipificado como infracción grave en el artículo 44.3 b) de la Ley Orgánica. Asimismo, es infracción grave el tratamiento de las imágenes más allá de los límites temporales de conservación legalmente previsto, por su poner una conculcación del artículo 4.5 de la Ley Orgánica, sancionable conforme a su artículo 44.3 c) que tipifica como infracción “Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave”.

Finalmente, la revelación de las informaciones obtenidas en el desempeño de funciones de seguridad privada si dichas informaciones contienen datos de carácter personal implica una vulneración del deber de secreto al que se refiere el artículo 10 de la Ley Orgánica 15/1999 y tipificada como infracción grave por el artículo 44.3 d) de la misma.

Se plantea así el problema de que una misma acción puede resultar constitutiva de diversas infracciones tipificadas en la normativa reguladora de la protección de datos y la que establece el régimen de la seguridad privada, planteándose así una posible vulneración del principio “non bis in idem” o un supuesto en el que las autoridades competentes en las materias reguladas por el Anteproyecto declararían infracciones que realmente lo son de la Ley Orgánica 15/1999, quedando así vedada la garantía del derecho fundamental a tribuido a esta Agencia.

A nuestro juicio, partiendo del hecho de que en ambas normas se está haciendo referencia al tratamiento o uso ilícito de datos de carácter personal, debe entenderse que debe prevalecer la aplicación de los tipos sancionadores establecidos en la Ley Orgánica 15/1999, dado su carácter de Ley especial reguladora de la materia y referida específicamente a la garantía de una derecho fundamental.

Ciertamente esta Agencia es consciente que el catálogo de sanciones contenido en el artículo 45 de la Ley Orgánica 15/1999 no contiene sanción alguna en relación con la revocación o suspensión temporal de la habilitación, en los términos establecidos en los artículos 60 y 61 del Anteproyecto sometido a informe, no siendo en modo alguno competente para imponer este tipo de sanciones. Pero ello no puede implicar, a nuestro juicio, el reconducir tipos infractores que se refieren al tratamiento ilícito de datos de carácter personal al elenco contenido en los artículos 56 y 57 del Anteproyecto.

A tal efecto, sería posible el establecimiento de un sistema de coordinación entre ambas normas que permitiese el reenvío por parte de esta Agencia a los órganos competentes en materia sancionadora, enumerados en el artículo 65 por conducto del Ministerio del Interior de las sanciones impuestas por la comisión de las conductas ahora tipificadas por el Anteproyecto a fin de que por aquél, o por los órganos competentes en su caso dentro de la estructura del Departamento (en este caso, el Secretario de Estado de Seguridad y el Director General de la Policía) se impusieran, si resultase pertinente, las sanciones de revocación o suspensión temporal de la habilitación mediante el correspondiente procedimiento sancionador, teniendo como probados los hechos declarados como tales por la resolución de la Agencia que hubiera impuesto la correspondiente sanción.

De este modo, se propone, en primer lugar, la supresión de los tipos mencionados con anterioridad en el presente apartado de este informe, lo que supondría:

- **La supresión íntegra de los contenidos en los artículos 56.1 j), 56.2 m) y 57.2 g),**

- **La modificación de los establecidos en los artículos 56.1 c) y 57.1 g), omitiendo la referencia al "mantenimiento de ficheros, automatizados o no, de datos de carácter personal e información a terceras personas sobre clientes, personas relacionadas con éstos", de forma que se sanciones por dichos tipos la realización de las actividades prohibidas por el artículo 8.5 salvo que ello suponga la vulneración de la normativa de protección de datos de carácter personal.**

- **La modificación del artículo 57.1 g) del Anteproyecto en el sentido de señalar que es infracción la vulneración del deber de reserva salvo que ello sea constitutivo de infracción en materia de protección de datos de carácter personal.**

A su vez, **sería preciso que el Anteproyecto estableciese que en los supuestos en que la Agencia Española considere que se ha producido un tratamiento de datos de carácter personal que constituya una de las actividades prohibidas por el artículo 8.5 de la Ley, así como cuando se haya producido la vulneración por el personal de seguridad del deber de secreto establecido en la Ley Orgánica 15/1999 y en todo caso cuando se haya producido el tratamiento por las empresas de seguridad de datos de carácter personal como consecuencia de la instalación de sistemas de videovigilancia o por sistemas de alarma que no reúnen los requisitos establecidos en la Ley o las imágenes o los datos obtenidos por detectives privados sean conservados más allá de los plazos establecidos en la misma, la Agencia dará traslado al Ministerio del**

Interior de la resolución a fin de que el mismo o los órganos de aquél que resulten competentes determinen la procedencia de imponer a la empresa o al personal de seguridad las sanciones no pecuniarias establecidas en los artículos 61 y 62 del Anteproyecto.