

N/REF: 133330/2017

Se plantea si resulta conforme a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, los tratamientos de datos personales que se efectúen en el marco de las actividades del proyecto europeo SURVANT, incluido en el ámbito del programa Horizonte 2020 de la Unión Europea.

Según la documentación aportada el proyecto tiene como objetivo desarrollar un sistema de análisis de video para automatizar los procedimientos de videovigilancia. En el marco de dicho proyecto se señala que se utilizarán las grabaciones de las cámaras que la Policía Municipal participante en el proyecto tiene en la vía pública. En particular, se mencionan las videocámaras instaladas en sus vehículos controladas por un centro de integrado de emergencias y seguridad, los accesos a videocámaras que regulan el control del tráfico y el acceso a videocámaras instaladas en transportes públicos como autobuses y metro.

En el proyecto participa un ente público español y diversas entidades de países miembros de la Unión Europea.

I

La primera cuestión que plantea el proyecto es la de la aplicabilidad de la normativa de protección de datos. A este respecto, debe indicarse que, con carácter general, los artículos 1 y 2 de la Ley Orgánica 15/1999 extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la citada Ley como *“cualquier información concerniente a personas físicas identificadas o identificables.”*

El artículo 5.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, precisa que constituye un dato de carácter personal *“Cualquier información numérica,*



alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.”

En consecuencia, tanto la imagen como la voz de una persona identificada o identificable constituyen datos de carácter personal, por lo que su tratamiento está sujeto a lo previsto en la normativa de protección de datos. Asimismo, conforme a la definición del artículo 5 arriba transcrito, esa calificación se extiende a otras informaciones, como las matrículas de los vehículos que circulen por la calle, que igualmente pueden ser captadas con las cámaras. En este sentido, el informe de esta Agencia de 8 de febrero de 2007 recordaba el carácter de dato personal que las matrículas de los vehículos pueden tener y, en consecuencia, la sumisión a la Ley Orgánica 15/1999 del tratamiento de dicho dato. Se señalaba en el mismo que, siguiendo el criterio sustentado por las distintas Recomendaciones emitidas por el Comité de Ministros del Consejo de Europa, en las que se indica que la persona deberá considerarse identificable cuando su identificación no requiere plazos o actividades desproporcionados, debe concluirse que las placas de matrícula constituyen un dato personal por reunir dichas características, ya que la identificación del titular de los vehículos cuya matrícula sea conocida, únicamente exigirá la consulta del Registro de Vehículos, al que se refiere el Reglamento General de Vehículos, aprobado por Real Decreto 2822/1998, de 23 de diciembre, cuya finalidad esencial es la identificación del titular, para lo cual únicamente será necesaria la invocación del interés legítimo del solicitante.

Debe, asimismo, hacerse referencia al concepto de tratamiento de datos personales, toda vez que de lo expuesto en el proyecto se desprende la realización de diversos posibles tratamientos. A este respecto, constituye un tratamiento de datos, conforme a lo establecido en el artículo 3.c de la Ley Orgánica 15/1999, las *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.”*

Por consiguiente, la realización de alguna o varias de estas operaciones respecto de datos personales constituirá un tratamiento de datos personales. Debe así tenerse en cuenta que la recogida de datos no constituye el único tratamiento posible, sino que otras operaciones (por ejemplo, conservación, elaboración, modificación o comunicaciones de datos) constituyen también tratamientos de datos personales y son igualmente determinantes, de la aplicabilidad de la normativa de protección de datos.

No obstante, debe tenerse en cuenta que no resulta aplicable la normativa de protección de datos cuando no sea posible identificar a las personas, por haberse sometido sus datos a un proceso de disociación; la Ley Orgánica 15/1999 describe éste en su artículo 3 f) como *“Todo tratamiento de*



datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.”

Conforme al artículo 5.1.o del Reglamento de desarrollo de la Ley Orgánica 15/1999 es identificable *“toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.”*

Dicha definición tiene su origen en lo dispuesto en el artículo 2 de la aludida Directiva 95/46/CE, conforme al cual son datos personales *“toda información sobre una persona física identificada o identificable (el “interesado”); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social»*. Asimismo, tiene en cuenta el considerando 26 de dicha Directiva 95/46/CE en el que se señala que con el fin de *“determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona”*.

Por parte de esta Agencia se ha venido señalando que para que un procedimiento de disociación pueda ser considerado suficiente a los efectos de la Ley Orgánica 15/1999, es necesario que de la aplicación de dicho procedimiento resulte imposible asociar el dato o datos de que se disponga a un sujeto determinado. Para ello será preciso que no exista la posibilidad, incluso remota, de que, mediante la utilización, con carácter previo, coetáneo o posterior de cualquier medio, la información concerniente a los afectados por el tratamiento de datos, que obre en poder del consultante, pueda revelar su identidad.

En esta materia resulta de especial interés lo señalado en sus Dictámenes por el Grupo de Trabajo del artículo 29, órgano consultivo independiente de la Unión Europea sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Así ya en su Dictamen 6/2013 indicaba que *“La anonimización es cada vez más difícil de lograr con el avance de las modernas tecnologías informáticas y la disponibilidad de la información de forma ubicua. La reidentificación de las personas es cada vez más común y representa una amenaza en la actualidad. En la práctica, existe una importante zona gris, en la que el responsable del tratamiento de datos puede creer que un conjunto de datos está anonimizado,*



pero un tercero puede ser capaz de identificar al menos a algunas personas a partir de estos datos, por ejemplo, utilizando otros datos públicos o cualquier otra información de que disponga.”

En particular en el Dictamen 5/2014, sobre técnicas de anonimización, el citado Grupo de Trabajo señalaba que *“A la luz de la Directiva 95/46/CE y de otros instrumentos jurídicos pertinentes de la UE, la anonimización es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación.”*

Se recordaba en dicho Dictamen 5/2014 que *“El Grupo de Trabajo examinó el concepto de «datos personales» en el Dictamen 4/2007 sobre datos personales, en el que se centra en los elementos componentes de la definición del artículo 2, letra a), de la Directiva 95/46/CE, entre ellos la referencia a una persona física «identificada o identificable». En este contexto, el Grupo de Trabajo llegó a la conclusión de que «los datos anonimizados serían, por tanto, datos anónimos que antes hacían referencia a una persona identificable, pero que ahora ya no admiten identificación».*

Por consiguiente, el Grupo de Trabajo ya ha aclarado que la Directiva propone la razonabilidad de los medios usados («el conjunto de los medios que puedan ser razonablemente utilizados») como criterio para evaluar si el tratamiento de anonimización es suficientemente sólido, es decir, si la identificación es «razonablemente» imposible. Afectan directamente a la identificabilidad el contexto y las circunstancias particulares de cada caso.

(...) Una solución de anonimización eficaz impide a todos singularizar a una persona en un conjunto de datos, vincular dos registros en un conjunto de datos (o dos registros pertenecientes a conjuntos diferentes) e inferir cualquier tipo de información a partir de dicho conjunto. En definitiva, como norma general, no basta con eliminar los elementos que pueden servir para identificar directamente a una persona para garantizar que ya no se puede identificar al interesado. Con frecuencia habrá que tomar medidas adicionales para evitar dicha identificación, las cuales dependerán una vez más del contexto y de los fines del tratamiento de que van a ser objeto los datos.”

En dicho Dictamen 5/2014 se ponía igualmente de manifiesto que *“Es importante dejar claro que el concepto de «identificación» no conlleva únicamente la posibilidad de recuperar el nombre o la dirección de una persona, sino que incluye también la identificabilidad potencial por singularización, vinculabilidad o inferencia. Es más, a efectos legales es irrelevante la intención del responsable del tratamiento o del destinatario. Mientras los datos sean identificables, se aplica la legislación sobre protección de datos.”*



Debe así señalarse que no sería de aplicación la normativa de protección de datos en el supuesto de que se llevase a cabo una efectiva anonimización previa de todas y cada una de las imágenes a tratar durante la ejecución del proyecto de modo que fuera imposible identificar a las personas captadas con las cámaras o las matrículas de los vehículos. En el presente supuesto se hace referencia en la documentación al ocultamiento o eliminación de la identidad de los afectados por el tratamiento (por ejemplo, difuminando rostros) u otras características reconocibles (matrículas de vehículos) en origen, sin embargo, en otras partes del documento se hace referencia al uso de esquemas de anonimización selectiva que permitirán que solamente se conserven los datos personales relevantes, siendo esto último más coherente con la finalidad del proyecto, en tanto que los sistemas de videovigilancia persiguen identificar al autor o autores de los hechos delictivos y el proceso de automatización de las búsquedas en los videos tiene como objetivo facilitar dicha identificación. Por consiguiente, en tanto el proceso de anonimización en origen no se emplee con todas las imágenes que contienen datos personales, la aplicación de la normativa de protección de datos no queda excluida.

II

La segunda cuestión que plantea el supuesto es la relativa a la normativa aplicable al tratamiento de los datos con fines de investigación científica señalado en la consulta.

Como punto de partida cabe recordar que la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, excluía, en su artículo 3.2, de su ámbito de aplicación el tratamiento de datos personales *“efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal”*

En este sentido el considerando 16 de la aludida Directiva venía a señalar que “los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, no están comprendidos en el ámbito de aplicación de la presente Directiva cuando se aplican con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con ámbitos del derecho penal o para el ejercicio de otras

actividades que no están comprendidos en el ámbito de aplicación del Derecho comunitario”

El tratamiento de datos personales con tales finalidades se rige por las leyes nacionales que, a juicio de esta Agencia, igualmente determinarán los posibles usos ulteriores, cautelas y garantías a que están sujetos tales datos.

En el ámbito del derecho español actualmente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal regula en su artículo 22 los ficheros de las Fuerzas y Cuerpos de Seguridad distinguiendo entre aquéllos que contengan datos recogidos para fines administrativos, que quedarán sujetos al régimen general previsto en dicha Ley, y los que sirvan para fines de investigación policial, sometidos a un régimen diferenciado contenido en sus artículos 22.2 y siguientes. En lo que respecta a la captación de imágenes y sonidos con cámaras de videovigilancia por las Fuerzas y Cuerpos de Seguridad, la Ley Orgánica 15/1999, en su artículo 3.e), remite a su legislación específica constituida por la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y su Reglamento de desarrollo, aprobado por Real Decreto 596/1999, de 16 de abril, resultando de aplicación supletoria la Ley Orgánica 15/1999 en lo no previsto por la citada legislación específica.

Ahora bien, debe tenerse en cuenta que a partir de 25 de mayo de 2018 resultará de aplicación el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que desplaza la aplicación de la Ley Orgánica 15/1999 en los aspectos regulados por dicho Reglamento. No obstante, el aludido Reglamento excluye de su ámbito de aplicación en su artículo 1.2.d) el tratamiento de datos personales *“por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.”* La regulación de los tratamientos personales con tal finalidad viene recogida en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

La citada Directiva (UE) 2016/680, prohíbe en su artículo 9 el uso de tales datos recogidos por las autoridades competentes para otros fines distintos a los enumerados en su artículo 1 apartado 1, esto es, la prevención,



investigación detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la protección y la prevención frente a las amenazas contra la seguridad pública, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión o del Estado miembro. No obstante, su artículo 4 habilita un uso científico de los datos cuando su finalidad sea igualmente la establecida en el artículo 1, apartado 1 de la Directiva. Dispone el artículo 4 de dicha norma lo siguiente:

“2. Se permitirá el tratamiento de los datos personales, por el mismo responsable o por otro, para fines establecidos en el artículo 1, apartado 1, distintos de aquel para el que se recojan en la medida en que:

a) el responsable del tratamiento esté autorizado a tratar dichos datos personales para dicho fin de conformidad con el Derecho de la Unión o del Estado miembro, y

b) el tratamiento sea necesario y proporcionado para ese otro fin de conformidad con el Derecho de la Unión o del Estado miembro.

3. El tratamiento por el mismo responsable o por otro podrá incluir el archivo en el interés público, el uso científico, estadístico o histórico para los fines establecidos en el artículo 1, apartado 1, con sujeción a las salvaguardias adecuadas para los derechos y libertades de los interesados.”

El supuesto objeto de consulta se encuadraría en un futuro en lo previsto en el número 3 de tal precepto toda vez que su finalidad es facilitar las investigaciones policiales automatizando los procedimientos de vigilancia utilizando soluciones de análisis de video y que se lleva a cabo por la propia entidad legitimada para el tratamiento de los datos con fines policiales.

En consecuencia, la regulación actual de tales tratamientos viene constituida por la Ley Orgánica 15/1999; por la Ley Orgánica 4/1997 y por sus respectivas normativas de desarrollo, que continuarán siendo de aplicación a los tratamientos a llevar a cabo en el proyecto hasta tanto entre en vigor la normativa nacional que desarrolle la directiva 2016/680, sin que al tratamiento con fines de investigación científica objeto de consulta le resulte de aplicación lo previsto en el Reglamento UE/679/2016 aun cuando la ejecución de proyecto se prolongue a un período posterior a 25 de mayo de 2008.

III

En aplicación de lo previsto en la ley Orgánica 15/1999 para que un tratamiento de datos personales sea lícito será preciso que el responsable se encuentre legitimado en la forma prevista en su artículo 6 conforme al cual *“el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.”* No obstante, el



número segundo de dicho precepto dispone que *“No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias.”* La consulta se refiere a la utilización de las imágenes captadas con las videocámaras instaladas en los vehículos de la policía municipal que son controladas por un centro integrado de emergencias y seguridad del Ayuntamiento, a las captadas con videocámaras que regulan el control del tráfico y a las captadas con videocámaras instaladas en transportes públicos como autobuses o metro a que tiene acceso la policía, por lo que antes de analizar si procede su uso con fines de investigación científica, debe hacerse una referencia previa a la legitimación para el tratamiento de tales imágenes por parte del consultante con fines de policiales.

Así, en primer lugar, la consulta señala que se utilizarán las imágenes grabadas con cámaras instaladas en los vehículos de la policía. La utilización de cámaras con fines de videovigilancia a efectuar por las Fuerzas y Cuerpos de Seguridad, como se ha señalado, se encuentra regulada en Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y su Reglamento de desarrollo, aprobado por Real Decreto 596/1999, de 16 de abril y se encuentra sujeta a muy estrictos requisitos por dicha Ley.

Debe recordarse que las instalaciones fijas de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado y de las Corporaciones Locales exigen la autorización del Delegado del Gobierno en la Comunidad Autónoma de que se trate, previo informe de una Comisión cuya presidencia corresponderá al Presidente del Tribunal Superior de Justicia de dicha Comunidad, tal y como prevé el artículo 3 de la Ley Orgánica 4/1997. El número 4 del artículo 3 regula el contenido de dicha autorización disponiendo que *“La resolución por la que acuerde la autorización deberá ser motivada y referida en cada caso al lugar público concreto que ha de ser objeto de observación por las videocámaras. Dicha resolución contendrá también todas las limitaciones o condiciones de uso necesarias, en particular la prohibición de tomar sonidos, excepto cuando concurra un riesgo concreto y preciso, así como las referentes a la cualificación de las personas encargadas de la explotación del sistema de tratamiento de imágenes y sonidos y las medidas a adoptar para garantizar el respeto de las disposiciones legales vigentes. Asimismo deberá precisar genéricamente el ámbito físico susceptible de ser grabado, el tipo de cámara, sus especificaciones técnicas y la duración de la autorización, que tendrá una vigencia máxima de un año, a cuyo término habrá de solicitarse su renovación.”*

En lo que respecta a la autorización de videocámaras móviles hay que estar a lo dispuesto en el artículo 5 de dicha Ley según el cual:

“1. En las vías o lugares públicos donde se haya autorizado la instalación de videocámaras fijas, podrán utilizarse simultáneamente otras de carácter móvil para el mejor cumplimiento de los fines previstos en esta Ley, quedando, en todo caso, supeditada la toma, que ha de ser conjunta, de

imagen y sonido, a la concurrencia de un peligro concreto y demás requisitos exigidos en el artículo 6.

2. También podrán utilizarse en los restantes lugares públicos videocámaras móviles. La autorización de dicho uso corresponderá al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización del medio a los principios previstos en el artículo 6.

La resolución motivada que se dicte autorizando el uso de videocámaras móviles se pondrá en conocimiento de la Comisión prevista en el artículo 3 en el plazo máximo de setenta y dos horas, la cual podrá recabar el soporte físico de la grabación a efectos de emitir el correspondiente informe.

En casos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización indicada en razón del momento de producción de los hechos o de las circunstancias concurrentes, se podrán obtener imágenes y sonidos con videocámaras móviles, dando cuenta, en el plazo de setenta y dos horas, mediante un informe motivado, al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y a la Comisión aludida en el párrafo anterior, la cual, si lo estima oportuno, podrá requerir la entrega del soporte físico original y emitir el correspondiente informe.

En el supuesto de que los informes de la Comisión previstos en los dos párrafos anteriores fueran negativos, la autoridad encargada de la custodia de la grabación procederá a su destrucción inmediata.

3. La Comisión prevista en el artículo 3 será informada quincenalmente de la utilización que se haga de videocámaras móviles y podrá recabar en todo momento el soporte de las correspondientes grabaciones y emitir un informe al respecto.

4. En el caso de que las autoridades competentes aludidas en esta Ley lo consideren oportuno, se podrá interesar informe de la Comisión prevista en el artículo 3 sobre la adecuación de cualquier registro de imágenes y sonidos obtenidos mediante videocámaras móviles a los principios del artículo 6.”

Por su parte, el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, aprobado por Real Decreto 596/1999, de 16 de abril, se refiere en sus artículos 6 a 9 al procedimiento de autorización de videocámaras móviles, señalando los órganos competentes tanto para solicitar como para conceder la autorización precisa para su utilización.

Así en lo que respecta a su solicitud dispone el artículo 6 del citado Reglamento “1. Podrán formular la solicitud los mandos operativos de las Fuerzas y Cuerpos de Seguridad del Estado por el conducto reglamentario y el Alcalde o el concejal competente en materia de seguridad ciudadana, respecto a la policía local de su municipio.



2. La solicitud, que deberá acreditar la necesidad e idoneidad del uso de este tipo de videocámaras, se dirigirá a los órganos señalados en el artículo siguiente.”

El artículo 7 señala la competencia para la autorización previendo que *“1. En las Comunidades Autónomas uniprovinciales y en las provincias donde tenga su sede la Delegación del Gobierno, la autorización del uso de videocámaras móviles corresponderá al Delegado del Gobierno.*

2. La autorización del uso de videocámaras móviles corresponderá al Subdelegado del Gobierno en aquellas provincias donde no radique la sede de la Delegación del Gobierno.”

El artículo 8 dispone lo siguiente respecto de la resolución de las solicitudes formuladas:

1. En el plazo máximo de un mes, contado a partir del día siguiente al de la presentación de la solicitud, se notificará la resolución motivada de acuerdo con lo previsto en el artículo cuarto de la Ley Orgánica 4/1997.

Si la resolución es autorizatoria, se pondrá en conocimiento de la Comisión de Garantías de la Videovigilancia correspondiente en el plazo máximo de setenta y dos horas a contar desde su adopción, por cualquier medio telemático, informático o documental que acredite su recepción.

2. Si transcurrido el citado plazo de un mes no se hubiese dictado resolución, la autorización se entenderá desestimada.

3. La resolución del Delegado del Gobierno pondrá fin a la vía administrativa y contra la misma cabrá interponer potestativamente recurso de reposición o impugnarla directamente ante el orden jurisdiccional contencioso-administrativo. Contra la resolución del Subdelegado del Gobierno podrá interponerse recurso de alzada ante el Delegado del Gobierno.”

Por último el artículo 9 se refiere al régimen excepcional previsto en el párrafo tercero del artículo 5.2 de la Ley Orgánica 4/1997, disponiendo que en tal supuesto *“las Fuerzas y Cuerpos de Seguridad que realicen las grabaciones, lo comunicarán, en el plazo de veinticuatro horas, a la autoridad contemplada en el artículo 7 de este Reglamento, y en las siguientes veinticuatro horas le remitirán ineludiblemente un informe motivado al respecto.*

Dicha autoridad, en el plazo máximo de setenta y dos horas desde que se realizó la grabación, lo pondrá en conocimiento de la Comisión de Garantías de la Videovigilancia correspondiente, remitiéndose, además, el aludido informe motivado.”

La Ley Orgánica 4/1997, exige además que se adopte un criterio de proporcionalidad en la utilización de las cámaras, disponiendo el artículo 6 de la misma al respecto lo siguiente:

“1. La utilización de videocámaras estará presidida por el principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima.



2. La idoneidad determina que sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en esta Ley.

3. La intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas.

4. La utilización de videocámaras exigirá la existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles.

5. No se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni de los lugares incluidos en el artículo 1 de esta Ley cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Las imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia.”

Por consiguiente el uso de las cámaras móviles por la policía municipal a que hace referencia la consulta, solamente podrá llevarse a cabo en los casos y con los requisitos hasta aquí transcritos, teniendo en cuenta el carácter de excepcionalidad con que las normas reguladoras de la materia contemplan la adopción de dicha medida.

Uno de los de los aspectos esenciales del tratamiento de datos captados por las cámaras, fijas o móviles, por parte de las Fuerzas y Cuerpos de Seguridad es el de la finalidad de las grabaciones, determinada en el artículo 7 de la Ley Orgánica 4/1997, según el cual

“1. Realizada la filmación de acuerdo con los requisitos establecidos en la Ley, si la grabación captara la comisión de hechos que pudieran ser constitutivos de ilícitos penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad a disposición judicial con la mayor inmediatez posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.

2. Si la grabación captara hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad ciudadana, se remitirán al órgano competente, igualmente de inmediato, para el inicio del oportuno procedimiento sancionador.”

Si las imágenes grabadas no captan hechos constitutivos de ilícitos penales o infracciones administrativas relacionadas con la seguridad ciudadana deberán ser destruidas, tal y como dispone el artículo 8 de la Ley, a cuyo tenor *“1. Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o*



administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.”

De este modo las imágenes obtenidas no pueden quedarse almacenadas sino que deben ser destruidas si no captan delitos o infracciones graves o muy graves en materia de seguridad o puestas a disposición judicial, salvo que se utilicen en el marco de una investigación policial en curso o de un procedimiento judicial o administrativo abierto. En tales casos las imágenes que no deban ser destruidas pasarán a formar parte de otro tipo de ficheros, sean los creados para la instrucción y sanción de infracciones administrativas, sean judiciales o sean policiales cuando se trate de imágenes relacionadas con una investigación policial, estos últimos son los regulados en los artículos 22.2 y siguientes de la Ley Orgánica 15/1999.

Dispone el artículo 22.2 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”*. El artículo 23 limita la recogida y tratamiento de los datos especialmente protegidos a que se refiere el artículo 7 números 2 y 3 a los casos en que sea *“absolutamente necesario para los fines de una investigación concreta.”* Y el artículo 24 establece una norma específica para la cancelación de los datos contenidos en los ficheros a los que se viene haciendo referencia al disponer que *“Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.”*

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.”

El régimen especial de los ficheros policiales, además de incluir determinadas limitaciones respecto a los derecho de acceso, rectificación, cancelación y oposición de los interesados reguladas en los artículos 23 y 24 de la Ley Orgánica 15/1999, exige que estos ficheros se encuentren sujetos a medidas de seguridad de nivel alto, tal y como dispone el artículo 81.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999, según el cual *“Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.”*



En lo que respecta al uso de las cámaras de vigilancia del tráfico, la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos regula en su disposición adicional octava las cámaras instaladas en la vía pública para vigilancia del tráfico disponiendo que *“La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico se efectuará por la autoridad encargada de la regulación del tráfico a los fines previstos en el texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto legislativo 339/1990, de 2 de marzo, y demás normativa específica en la materia, y con sujeción a lo dispuesto en las Leyes Orgánicas 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y 1/1982, de 5 de mayo, de Protección Civil del derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, en el marco de los principios de utilización de las mismas previstos en esta Ley.”*

El Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, establece en su disposición adicional única, el régimen aplicable a las videocámaras para la vigilancia, control y disciplina del tráfico, señalando en su apartado 7 que *“La utilización de las videocámaras contempladas en esta disposición por las Fuerzas y Cuerpos de Seguridad para fines distintos de los previstos en la misma se regirá por lo dispuesto en la Ley Orgánica 4/1997 y en el presente Reglamento.”* Si bien señala que *“en el caso de que dicha utilización se realice por las Unidades de Policía Judicial en sentido estricto, se estará a lo dispuesto en la Ley de Enjuiciamiento Criminal y en su normativa específica.”*

Por consiguiente, el uso de las imágenes captadas por las cámaras de vigilancia de tráfico con la finalidad de seguridad no se incardina en el *“el control, regulación, vigilancia y disciplina del tráfico”* a que se refiere la disposición final octava de la Ley Orgánica 4/1997, sino en lo previsto en el artículo primero de dicha Ley respecto a la prevención de la comisión de infracciones, faltas y delitos relacionados con la seguridad pública, debiendo ajustarse su utilización a lo previsto en dicha Ley para tales supuestos. Asimismo, tales imágenes cuando se utilicen en el marco de una investigación policial pasarán a formar parte del correspondiente fichero policial a que se refiere el artículo 22.2 de la Ley Orgánica 15/1999 cuyo régimen jurídico se ha examinado.

En tercer lugar en lo que respecta al acceso a las imágenes captadas con videocámaras en los sistemas de transporte público, metro y autobuses, su legitimación se encuentra en la actualidad en lo previsto en el artículo 15.1 de la Ley 5/2014, de 4 de abril, de Seguridad Privada conforme al cual *“ Se autorizan las cesiones de datos que se consideren necesarias 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.”

Ahora bien, dicha norma no constituye una autorización general que permita cualquier acceso en cualquier momento a tales ficheros sino que tal acceso viene limitado a los supuestos fijados en el propio precepto, supuestos que coinciden con los establecidos para la creación de ficheros policiales en el artículo 22 de la Ley Orgánica 15/1999 y debe reunir los requisitos establecidos en la normativa de protección de datos, a la que se remite el mismo precepto en su número segundo al disponer 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.”

Esta Agencia examinó en informe de 23 de mayo de 2014 la conformidad de diversas modalidades de acceso a tales datos, siempre que se diera cumplimiento al principio de proporcionalidad, señalando, en primer lugar que tal principio viene a exigir los siguientes requisitos:

- “a) Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.
- b) Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.
- c) Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.
- d) Que, en cumplimiento del artículo 22.4 de la Ley Orgánica 15/1999, los datos sean cancelados “cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento”.

Se señalaba así la conformidad con tal principio de los accesos en tiempo real a las imágenes de sistemas de videovigilancia instalados en los autobuses públicos cuando el conductor acciona el dispositivo de emergencias, considerando que parecía resultar ajustado a los requisitos señalados en los informes de esta Agencia para concretar el principio de proporcionalidad en el supuesto de acceso a datos por parte de las Fuerzas y Cuerpos de Seguridad, en particular, en lo que respecta a la exigencia de una petición concreta y específica y que sea además necesaria para la prevención de un peligro real y



grave para la seguridad pública o para la represión de infracciones penales quedando debidamente acreditada la relación del acceso a las imágenes con dichos supuestos de hecho

Igualmente señalaba dicho informe, en lo que respecta a la puesta a disposición de la policía municipal de las grabaciones efectuadas por los sistemas de videovigilancia instalados en los autobuses públicos relacionadas con la comisión de un delito que hubiera sido objeto de denuncia por un ciudadano, que la comunicación de las imágenes en que se constataste la comisión del delito, efectuada tras una petición individualizada y motivada por parte de la policía, sería conforme a dicho principio. De la misma manera, en aquellos supuestos en que el responsable del fichero constataste la comisión de un delito público flagrante, que se encuentra obligado a denunciar, la puesta a disposición de la policía de las grabaciones en las que queda reflejada la acción constitutiva del delito sería igualmente conforme al principio de proporcionalidad.

En los demás supuestos en los que la visualización no tiene como objetivo la comprobación de la existencia de un delito ya cometido o que se está produciendo, sino su posible prevención, señalaba esta Agencia lo siguiente:

“En otros supuestos en que se habilita a las Fuerzas y Cuerpos de Seguridad a la captación de imágenes con fines de seguridad, como el previsto en la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, se establece una regulación que, como declara su exposición de motivos, introduce las garantías que son precisas para que el ejercicio de los derechos y libertades reconocidos en la Constitución sea máximo y no pueda verse perturbado con un exceso de celo en la defensa de la seguridad pública, sujetando dicha captación de imágenes a un régimen de autorización previa que requiere un informe previo preceptivo, que será vinculante si es negativo, de una comisión presidida por el Presidente del Tribunal Superior de Justicia de la Comunidad Autónoma de que se trate. Asimismo, permite el uso de videocámaras móviles con la necesaria autorización del máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad, salvo en situaciones de emergencia o en las que sea imposible obtener a tiempo la autorización, pero exigiendo en dicho caso comunicar su uso a la autoridad policial y a la Comisión, Comisión que será informada periódicamente del uso que se haga de videocámaras móviles y podrá recabar la correspondiente grabación.

No existiendo aquí un órgano al que se asigne específicamente la autorización o el control periódico de los accesos efectuados por la policía a las imágenes, debe partirse de los requisitos fijados por esta Agencia para la determinación de la proporcionalidad en el informe a que se viene



haciendo referencia, debiendo ponderarse en cada caso si el acceso a las imágenes resulta conforme a dicho principio:

De este modo, en aquéllos supuestos en que, como señala el consultante, con ocasión de un evento importante, una amenaza o un acto institucional, se establezca un dispositivo policial de seguridad, se podría considerar proporcional el acceso a las imágenes en tiempo real de determinadas líneas, siempre que quede acreditada la existencia de un peligro real y grave para la seguridad pública que justifique la adopción de dicha medida y que dicha medida sea limitada, dado que excede del principio de proporcionalidad una visualización general y masiva, delimitándose las líneas y el período de tiempo durante el que se considere que deba ejercerse la visualización en tiempo real. Dichas circunstancias deberán quedar documentadas.

En el supuesto mencionado por el consultante de vigilancia de líneas determinadas con ocasión de una investigación de carácter policial sin que medie requerimiento del Ministerio Fiscal o mandato judicial, no cabe tampoco una vigilancia masiva, debiendo quedar acreditada la comisión de delitos en la línea o líneas sobre las que vaya a establecerse la vigilancia, debiendo limitarse igualmente la visualización a dicha línea o líneas y por el tiempo estrictamente necesario para llevar a cabo las investigaciones policiales precisas para el esclarecimiento de los delitos, circunstancias que igualmente deberán quedar documentadas.”

Asimismo, dicho informe señalaba lo que a continuación se reproduce respecto de las medidas de seguridad a adoptar que conforman un segundo parámetro para determinar la proporcionalidad en el acceso a las imágenes captadas por el sistema de videovigilancia de la empresa pública de autobuses:

“Como segundo elemento que determina la proporcionalidad en el tratamiento de datos se encuentra el establecimiento de aquéllas medidas que garanticen que los accesos concretos a las imágenes captadas con el sistema de videovigilancia de la empresa consultante dan cumplimiento a dicho principio.

Señalaba a este respecto el Tribunal Constitucional en la aludida Sentencia 17/2013 respecto de la disposición adicional séptima de la Ley de Bases de Régimen Local, introducida por la Ley 14/2003 que



contempla el acceso por parte de la Dirección General de Policía a los datos sobre extranjeros contenidos en el Padrón municipal, en el ejercicio de sus competencias en la materia, y los requisitos exigibles: “Ahora bien, dicha previsión legal ha de ser entendida de forma acorde con las exigencias de proporcionalidad que nuestra doctrina exige en la limitación de un derecho fundamental como es el aquí concernido, relativo la protección de datos de carácter personal. Eso significa que la cesión de datos que el acceso regulado por el precepto supone ha de venir rodeado de una serie de garantías específicas, garantías que, cumplimentadas por el órgano administrativo al que el precepto hace referencia, son, evidentemente, susceptibles de control. Entre ellas se encuentra la necesidad de motivar y justificar expresamente tanto la concreta atribución de la condición de usuario para el acceso telemático a los datos del padrón que el precepto prevé, como los concretos accesos de que se trate, evitando —en cuanto que la exigible motivación de tales decisiones facilita su correspondiente control mediante los mecanismos previstos en el ordenamiento jurídico, en especial, a través del control jurisdiccional contencioso-administrativo— que se produzca tanto un uso torticero de dicha facultad como accesos indiscriminados o masivos. Límites al contenido del acceso que también resultan de determinadas previsiones de la legalidad ordinaria, las cuales han de ser aplicadas teniendo presente, en todo caso, la necesaria unidad del ordenamiento jurídico, tales como el art. 16.3 LBRL, que ya hemos examinado o, incluso, otras regulaciones específicas de la Ley Orgánica de protección de datos, en especial su art. 22.2. Resulta de ello que el acceso solamente será posible, en las condiciones antes dichas, cuando el concreto dato en cuestión resulte pertinente y necesario en relación con la finalidad que ha justificado el acceso, quedando garantizada la posibilidad de analizar si, en cada caso concreto, el acceso tenía amparo en lo establecido en la ley pues, en caso contrario, no resultará posible su uso. Con tales garantías el acceso regulado en la disposición cuestionada resulta ser proporcionado en relación con la finalidad perseguida, ya que, en tanto que el dato resultante solo puede ser utilizado para la finalidad establecida en el precepto, ha de realizarse de forma puntual por quien se encuentre expresamente habilitado para ello y en relación a datos concretos cuya necesidad ha de ser también justificada de forma expresa y, por tanto, sometida a control, en los términos que acabamos de exponer.”



Dichas garantías se corresponden con las medidas de seguridad exigibles para los ficheros y tratamientos de datos automatizados conforme al Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que si bien en el caso de la videovigilancia son de nivel básico, requerirán, a fines de garantizar en cada caso el cumplimiento del principio de proporcionalidad, algunas medidas de seguridad de nivel medio y alto. Dichas medidas serán diferentes en el caso en que se trate de accesos en tiempo real al sistema de videovigilancia del consultante o de la entrega de grabaciones.

Así en lo que respecta a los accesos en tiempo real, cabe recordar que el artículo 91 de dicho Reglamento exige que los usuarios tengan acceso únicamente a los recursos que precisen para el desarrollo de sus funciones, debiendo existir una relación actualizada de usuarios y perfiles de usuarios y los accesos autorizados para cada uno de ellos, así como mecanismos para evitar que un usuario acceda a recursos con derechos distintos de los autorizados. Dispone por último dicho artículo que en caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

El artículo 93 obliga al responsable del fichero a establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. Ello requiere que por parte de la policía se determine cuáles de sus miembros podrán acceder a las imágenes en tiempo real. Dichas personas tendrán la condición de usuarios del sistema del consultante y serán los únicos autorizados para acceder a las imágenes, debiendo el consultante establecer un mecanismo de identificación y autenticación que impida accesos no autorizados (pudiendo consistir en una contraseña en los términos del citado reglamento, u otros posibles como el de certificado electrónico).

Asimismo, deberá implementarse por parte de la policía un registro de accesos, en el que quedará registrado el usuario que accede, la cámara accedida, la fecha y la hora de comienzo y fin del acceso, lo que permitirá la efectiva comprobación de que el acceso se ha llevado a cabo de forma ajustada en cada caso al principio de proporcionalidad,



como señala el Alto Tribunal, y no se realizan accesos indiscriminados o masivos.

Por otra parte, dado que la visualización se efectúa en tiempo real, no cabe que las imágenes se incorporen a soportes distintos de los de la empresa consultante.

En lo que respecta a las entrega de grabaciones solicitadas por la policía municipal deberá establecerse como se hará entrega de las mismas, debiendo existir un sistema de salida de soportes en la entidad consultante, en los términos del artículo 97 del Reglamento citado y, paralelamente, un sistema de registro de entrada de soportes en la policía municipal, igualmente en los términos de dicho precepto.

Por otra parte, dichas grabaciones recibidas por la policía pasarán a formar parte de los ficheros con fines policiales a que se refiere el artículo 22 de la Ley Orgánica 15/1999, quedando sujetas a las prescripciones especiales que para los mismos contiene dicha Ley.”

Por consiguiente, solamente será conforme a lo establecido en la normativa de protección de datos el tratamiento de datos por parte del consultante cuando tales tratamientos se ajusten a los principios de finalidad y proporcionalidad señalados.

IV

Examinada la legitimación para el tratamiento con fines de seguridad y prevención de delitos de imágenes captadas con videocámaras que estará sujeta a los límites señalados, debe analizarse si tales datos, recabados conforme a las normas y con las garantías a que se ha hecho referencia, pueden ser utilizados con la finalidad de investigación científica a que la consulta se refiere.

El tratamiento de datos con fines policiales por los órganos competentes se encuentra sujeto al principio de finalidad contenido en el artículo 4.2 de la Ley Orgánica 15/1999, conforme al cual *“Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos”*. Debe aclararse que la Audiencia Nacional partiendo de una interpretación sistemática de este precepto viene considerando la expresión “finalidades incompatibles” como sinónimo de “finalidades distintas”.

De este modo no resultaría posible la utilización de los datos para una finalidad distinta a la prevista legalmente, sin el consentimiento del interesado o

sin que dicho tratamiento se encuentre legitimado en alguno de los supuestos contenidos en el artículo 6 de la Ley Orgánica 15/1999. No obstante, el propio artículo 4.2 de la Ley Orgánica 15/1999 dispone en su último inciso que *“No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.”*

En este mismo sentido dispone el Reglamento de desarrollo de la Ley Orgánica 15/1999 en su artículo 8.3 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”,* mientras que el artículo 9.1 prevé que *“No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.”*

Ahora bien, como tiene declarado esta Agencia en sus informes, no todo proyecto que se intitule como histórico, estadístico o científico tiene tal consideración, debiendo analizarse detenidamente y de forma individualizada si efectivamente a la vista del ente que desarrolla el estudio o investigación, el fin del mismo y la proporcionalidad de la intromisión o limitación del derecho a la protección de datos que el estudio conlleve, el tratamiento de datos resultante se encuentra amparado por lo previsto en los preceptos transcritos.

Dichas consideraciones toman como punto de partida que un tratamiento o cesión de datos personales constituye una limitación del derecho fundamental a la protección de datos de carácter personal, derecho que persigue garantizar a las personas, como ha declarado el Tribunal Constitucional en su Sentencia 292/2000, *“el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado”*. Debe así recordarse que conforme al artículo 53.1 la Constitución Española cualquier restricción de un derecho fundamental está sometida al principio de reserva de Ley y debe cumplir los principios de justificación y proporcionalidad

De este modo, en lo que se refiere al sentido que debe darse al término “científico”, finalidad en la que podría enmarcarse el proyecto objeto de la presente consulta, esta Agencia, en sus informes recordaba que la investigación científica y técnica, en el ámbito público, se encontraba regulada por la ahora derogada Ley 13/1986, de 14 de abril, de Fomento y Coordinación General de la Investigación, objetivo para el cual aquella establecía el Plan

Nacional de Investigación Científica y Desarrollo Tecnológico, pudiendo atribuirse la calificación de “científico” a aquellos proyectos insertos en el citado Plan.

Dicha conclusión se plasmó en el Reglamento de desarrollo de la Ley Orgánica 15/1999, que concreta en el segundo párrafo del artículo 9.1 el criterio que debe adoptarse para calificar la finalidad de un tratamiento como histórica, estadística o científica estableciendo que *“Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la [Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública](#), la [Ley 16/1985, de 25 junio, del Patrimonio histórico español](#) y la [Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica](#), y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.”*

Por consiguiente, para considerar que el tratamiento ulterior de los datos a que la consulta se refiere pudiera considerarse legitimado en una finalidad estadística o científica sería preciso que el estudio objeto de consulta estuviese considerado como estadística de cumplimentación obligatoria a los efectos previstos en la Ley 12/1989 o en la correspondiente Ley de estadística autonómica. Similar criterio debe adoptarse respecto al sentido que debe darse al término científico que podría amparar una investigación realizada con tales datos, dicha materia se encontraba regulada por la ahora derogada Ley 13/1986, de 14 de abril, de Fomento y Coordinación General de la Investigación, objetivo para el cual aquélla establecía el Plan Nacional de Investigación Científica y Desarrollo Tecnológico, pudiendo atribuirse la calificación de “científico” a aquellos proyectos insertos en el citado Plan. De modo equivalente cabría considerar como científico a los efectos del artículo 9 del Reglamento a una investigación enmarcada en alguno de los planes de investigación científica y técnica a que se refiere la vigente Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación o, en su caso, la correspondiente norma autonómica.

En cuanto a la legislación aplicable al presente caso, en que el consultante señala que el tratamiento de datos se llevaría a cabo en el marco de un proyecto del programa Horizonte 2020, vendría constituida por el Reglamento UE (nº 1291/2013 del Parlamento Europeo y del Consejo de 11 de diciembre de 2013 por el que se establece Horizonte 2020, Programa Marco de



Investigación e Innovación (2014-2020 y por el que se deroga la Decisión n o 1982/2006/CE. Por consiguiente, tratándose de un proyecto de I+D financiado por la Comisión Europea a través del aludido Programa Marco de Investigación e Innovación, cabe considerar que el tratamiento de los datos personales con el objetivo de desarrollar sistemas de análisis de video para automatizar los procesos de videovigilancia en el marco de dicho proyecto, puede ser calificado como científico a los efectos de encontrarse legitimado en lo previsto en la Ley Orgánica 15/1999.

Esta interpretación que permitiría el uso científico de los datos recogidos para fines policiales encuentra apoyo en lo previsto en la futura regulación de la materia, en tanto que la Directiva 2016/680, en su artículo 4, tal y como se ha señalado anteriormente, viene a habilitar el uso científico de los datos para los fines establecidos en su artículo 1, apartado 1.

V

El acceso a las imágenes captadas, formen parte de ficheros de videovigilancia o de ficheros policiales por personas o entidades distintas a las Fuerzas y Cuerpos de seguridad legitimadas para su tratamiento constituirá una cesión de datos personales definida en el artículo 3 i) de la Ley Orgánica 15/1999 como *“Toda revelación de datos realizada a una persona distinta del interesado”*.

El régimen general a que deben sujetarse las cesiones de datos viene recogido en el artículo 11 de la Ley Orgánica 15/1999, régimen que no resulta de aplicación a los datos especialmente protegidos. La Ley Orgánica 15/1999 incluye como datos especialmente protegidos aquellos a los que se refiere su artículo 7.5 según el cual *“Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas.”*

Debe tenerse aquí en cuenta que las imágenes captadas con fines de videovigilancia por las Fuerzas y Cuerpos de Seguridad y los datos incluidos en ficheros con fines policiales de los previstos en el artículo 22.2, solamente podrán ser cedidos en los casos legalmente establecidos, por lo que no cabe su comunicación a terceros, como serían los demás miembros del consorcio, sin la existencia de una previsión legal. No obstante, las demás entidades participantes en el consorcio podrían acceder a las imágenes en calidad de encargados del tratamiento del responsable. El artículo 12 de la Ley Orgánica



15/1999 regula la figura del encargado del tratamiento, disponiendo que *“No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.”*

En el marco del derecho español, para que la relación entre responsable y encargado del tratamiento pueda darse y se ajuste a la Ley, es preciso que se cumplan los requisitos expresados en el artículo 12 de la Ley Orgánica 15/1999, considerando los siguientes aspectos:

En primer lugar, es preciso que el acceso a los datos por el tercero se efectúe con la exclusiva finalidad de prestar un servicio al responsable del fichero, y que dicha relación de servicios se encuentre contractualmente establecida. En lo que atañe a los requisitos formales de este tipo de contratos, el artículo 12.2 de la Ley Orgánica 15/1999, impone que *“la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas”*.

El hecho de que la relación derivada del contrato sea la existente entre un responsable y un encargado del tratamiento implicará que al término de la relación sea aplicable lo establecido en el artículo 12.3 de la Ley Orgánica 15/1999, de forma que *“una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento”*.

El incumplimiento de esta previsión llevará aparejada la consecuencia, prevista en el artículo 12.4 de la citada Ley, de que *“En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente”*.

Esta Agencia Española de Protección de Datos ha venido indicando que el deber de devolución al que se refiere el artículo 12.3 de la aludida Ley Orgánica podrá verificarse mediante la entrega directa de los datos al propio responsable del tratamiento o mediante la realización de dicha entrega al encargado del tratamiento que este designase, toda vez que en este segundo caso el encargado actuaría como mero mandatario del responsable, siendo precisamente éste el que establece a quién han de entregarse los datos en su nombre y por su cuenta. Y así se recoge en el artículo 20.3 del Reglamento de



desarrollo de dicha Ley al disponer *“no obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.”*

Por su parte, el artículo 22 del aludido Reglamento dispone respecto de la conservación de los datos lo siguiente:

“1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.”

En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la Ley Orgánica 15/1999.

Por consiguiente, el instrumento jurídico en que se plasme el encargo del tratamiento debe ajustarse a las previsiones arriba transcritas, en otro caso, nos hallaríamos ante una cesión de datos carente de amparo legal.

VI

Entre las obligaciones del responsable e igualmente del encargado de tratamiento se encuentra la de adoptar las debidas medidas de seguridad. En este sentido cabe recordar que el artículo 9 de la Ley Orgánica 15/1999 dispone que *“El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.”*



El número 2 de dicho precepto prohíbe el registro de datos de carácter personal en ficheros *“que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.”*

Debe, además, recordarse que, como ha señalado reiteradamente la Audiencia Nacional en sus sentencias (por todas ellas SAN de 6-10-2011), la seguridad constituye una obligación de resultado consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros.

Las medidas de seguridad se encuentran reguladas en el Reglamento de desarrollo de la Ley Orgánica 15/1999 que constituye actualmente la normativa vigente en materia de medidas de seguridad y en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Los ficheros que contienen imágenes captadas con cámaras de videovigilancia están sujetos, con carácter general, a medidas de seguridad de nivel básico, si bien debe tenerse en cuenta que cuando tales imágenes pasan a formar parte de ficheros policiales de los previstos en el artículo 22.2 de la Ley Orgánica 15/1999 deberán aplicarse medidas de nivel alto. Dispone a este respecto el artículo 81.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999 que *“además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.”* Debe igualmente tenerse en cuenta que tal y como se desprende de dicho precepto las medidas de seguridad tienen un carácter acumulativo de modo de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores. Por otra parte, la necesaria proporcionalidad en el acceso a imágenes captadas con cámaras de terceros (transportes públicos) comportaba la adopción de mayores medidas de seguridad tal y como resultaba del análisis efectuado por esta Agencia respecto a su tratamiento al que se ha hecho referencia en el punto III de este informe.

Por consiguiente, las medidas de seguridad a aplicar durante el proyecto deberán respetar los requerimientos impuestos actualmente en materia de seguridad, sin perjuicio de que se incorporen mayores medidas de seguridad que puedan considerarse convenientes. Iguales medidas, como se ha señalado, deben adoptar los encargados de tratamiento. Por otra parte, las medidas exigibles en la actualidad pueden resultar modificadas si durante la ejecución del proyecto se aprobase la ley de desarrollo de la Directiva 2016/680, en los términos que aquella determine, debe tomarse en consideración, en particular, que dicha Directiva viene a imponer la implementación de un registro de operaciones para todos los ficheros incluidos en su ámbito de aplicación.



VII

Debe tenerse en cuenta que todo tratamiento de datos debe ser respetuoso de los principios relativos a la calidad de los datos recogidos en el artículo 4 de la Ley Orgánica 15/1999, debiendo destacarse en particular el de proporcionalidad, vinculado al principio de finalidad al que se hacía referencia en el punto III de este informe. Establece el artículo 4.1 de la Ley Orgánica 15/1999 a este respecto 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.”*

De este modo solamente podrán tratarse aquéllos datos que sean precisos para llevar a cabo las actividades objeto del proyecto. En la documentación se hace referencia a la utilización de técnicas de anonimización selectiva, que según se indica permitirán la conservación de solamente aquellos datos que sean relevantes, lo que cómo se ha señalado no implica la inaplicación de la normativa de protección de datos, pero dicha anonimización parcial debe valorarse positivamente al minimizar el tratamiento de datos a aquéllos precisos para llevar a cabo el proyecto.

Igualmente, dentro de los principios de calidad debe hacerse referencia al principio de conservación de los datos. El artículo 4.5 de la Ley Orgánica 15/1999 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.”*

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.”

En lo que respecta a los períodos durante los que deben ser conservados, debe tenerse en cuenta que el artículo 8 de la Ley Orgánica 4/1997, exige la destrucción de los datos recogidos a su amparo, en el plazo de máximo de un mes desde su captación, salvo que, como señala el mismo artículo, las grabaciones estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

En el caso de las grabaciones que hayan pasado a formar parte de ficheros policiales por estar relacionadas con infracciones penales o con una



investigación en curso, los plazos durante los cuales pueden conservarse las grabaciones son los señalados en el artículo 22 de la Ley Orgánica 15/1999, según el cual *“Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.*

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad”

Debe aquí tenerse en cuenta, que si bien la Ley Orgánica 4/1997 exige la destrucción de las grabaciones, la Ley Orgánica 15/1999 se refiere a la cancelación de los datos. La cancelación de los datos no supone la eliminación automática del dato, sino su bloqueo tal y como determina el artículo 16.3 de la Ley Orgánica 15/1999 al establecer que *“La cancelación 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. Cumplido el citado plazo deberá procederse a la supresión.”*

El Reglamento de desarrollo de la Ley Orgánica 15/1999, define en su artículo 5.1. b) la cancelación como *“Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.”*

En definitiva, el bloqueo consiste en que se impida el acceso a los datos por las personas que, en el marco de un tratamiento legítimo venían llevando éste a cabo, puesto que en el momento en que deba procederse a la cancelación de los mismos, sólo resultará lícita su utilización para su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales y con la única finalidad de atender a responsabilidades surgidas del tratamiento de datos. Así, esta Agencia entiende que para ello resulta preciso restringir el acceso a dichos datos, por cualquier procedimiento apto para conseguir ese resultado, a una persona con responsabilidad dentro de la organización del responsable.

Por consiguiente, deberán respetarse tanto por el responsable como por los encargados de tratamiento los plazos de destrucción de las grabaciones establecidos en la Ley Orgánica 4/1997 y los de cancelación establecidos en el artículo 22 de la Ley Orgánica 15/1999, lo que implica que no pueden



ampliarse tales plazos con motivo de proyecto de investigación objeto de consulta. En este sentido los encargados del tratamiento como se ha señalado deberán destruir o devolver las imágenes una vez cumplida la prestación contractual, sin que en ningún caso con motivo de la misma puedan superarse los plazos legalmente establecidos para la destrucción o cancelación de los datos. En lo que respecta a la previsión contenida en el Reglamento de desarrollo de la Ley Orgánica 15/1999 sobre el mantenimiento por el encargado de tratamiento de los datos bloqueados debe tenerse en cuenta que tal norma viene referida al plazo de garantía contractual. Tales plazos deben reflejarse en el instrumento jurídico en que se plasme el encargo de tratamiento.

VIII

Por último, debe reseñarse que en el presente supuesto, dentro de la prevención de posibles usos indebidos, se ha efectuado un análisis de riesgos valorando las amenazas y vulnerabilidades del sistema, teniendo en cuenta la posibilidad de que se pudieran producir usos internos malintencionados o accesos externos con fines delictivos o terroristas, considerando que tales actuaciones puede tener graves repercusiones en los derechos humanos, especialmente el relativo a la privacidad.

A efectos de mitigar tales riesgos se prevé, entre otras medidas, la de llevar a cabo una evaluación de impacto. Debe aquí señalarse que la realización de una evaluación de impacto relativa a la protección de datos debe valorarse positivamente como una buena práctica, ya que en el momento actual no resulta obligatoria conforme a la normativa vigente.

La Directiva 2016/680 señala un contenido mínimo para tal evaluación. En este sentido y sin perjuicio de la existencia de diversas metodologías existentes que pueden ser utilizadas, cabe indicar que el Grupo de Trabajo del Artículo 29 ha adoptado recientemente unas directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, que puede consultarse en el siguiente sitio web: (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083). Por su parte, esta Agencia ha publicado en su página web (www.agpd.es) una guía para las evaluaciones de impacto en la protección de datos sujetas al Reglamento General de Protección de Datos. Si bien ambas guías vienen referidas al Reglamento General de Protección de Datos y no a la Directiva 2016/680 parte de los aspectos que contemplan pueden constituir un referente para la realización de la evaluación de impacto.

Otra de las medidas hace referencia a la adopción de precauciones al publicar o difundir los resultados, sin que se concreten tales precauciones, debiendo recordarse que, en lo que respecta a los datos personales que pudieran tratarse en el proyecto, la comunicación o difusión de los mismos sin



causa legitimadora constituye una infracción de la normativa de protección de datos.