Informe 0344/2013

La consulta plantea si resulta conforme a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el acceso por parte de la Policía Municipal a las imágenes captadas por los sistemas de videovigilancia instalados en los autobuses de la entidad consultante. Se indica que, en la actualidad, existe un protocolo de trabajo entre ambos que consiste únicamente en el aviso telefónico de las incidencias que suceden a bordo de los autobuses de la flota.

Según expone el consultante, el sistema de videovigilancia graba continuamente durante el servicio las imágenes, que se guardan en un disco duro embarcado y, posteriormente, son descargadas en una central receptora de alarmas para su tratamiento si procede. En el caso de producirse una incidencia, el conductor acciona un pisón de emergencia que activa una alarma, que se recibe directamente en la central receptora de alarmas y que permite poner en marcha los mecanismos de seguridad que consisten, principalmente, en el aviso telefónico a la policía municipal para que se desplace al lugar de la incidencia. Con cada accionamiento del pisón de emergencias y la correspondiente señal de alarma se genera una imagen que puede ser puesta a disposición de la policía municipal.

Se plantea si resultarían ajustados a la normativa de protección de datos los siguientes supuestos de acceso por la policía municipal a las imágenes captadas por el sistema de videovigilancia de la entidad consultante:

1. Acceso por la policía municipal en tiempo real a las imágenes generadas por el sistema de videovigilancia, cuando la incidencia sea recogida por las cámaras al accionar el conductor el dispositivo de emergencias. Estas imágenes serían recibidas y valoradas previamente por la central receptora de alarmas y enviadas al centro integrado de señales de video de la policía para acordar el dispositivo de apoyo policial si este fuera necesario.

2. Poner a disposición de la policía municipal las grabaciones procedentes de las cámaras de los autobuses que estén relacionadas con una incidencia de seguridad concreta o con denuncias de ciudadanos relacionadas con hechos delictivos y que fueron grabadas con anterioridad a la petición.

3. Poner a disposición de la Policía municipal el visionado y grabación en tiempo real de las imágenes de líneas determinadas y muy específicas de autobuses, bien a instancias judiciales o por investigaciones de carácter policial que recojan claras evidencias delictivas.

4. Permitir que los servicios de policía municipal puedan visionar en tiempo real, las imágenes de aquellas líneas de autobuses que puedan verse afectadas por los dispositivos policiales de seguridad establecidos en la ciudad con motivo de importantes eventos, amenazas actos institucionales o cualquier otra situación que pudiera precisar un alto nivel de seguridad.

I

Las comunicaciones de datos a la que se refiere la consulta constituyen, conforme a lo dispuesto en el artículo 3 i) de la Ley Orgánica 15/1999, una cesión de datos de carácter personal, definida como "*Toda revelación de datos efectuada a persona distinta del interesado".*

Tal y como determina el artículo 11.1 de dicha Ley "*los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado".* Esta regla de consentimiento sólo se verá exceptuada en los supuestos contemplados en el número segundo de dicho artículo 11.2, de los que, en lo que se refiere al presente supuesto, cabe destacar aquellos casos en que una norma con rango de Ley dé cobertura a la cesión, previsto en su letra a) o cuando la comunicación tenga por destinatario el Ministerio Fiscal o los Jueces y Tribunales, contemplado en su letra d).

En lo que respecta a la comunicación de datos personales a las Fuerzas y Cuerpos de Seguridad, esta Agencia venía ya señalando en informe de 14 de junio de 2005 lo siguiente:

> "Deberán distinguirse aquellas actuaciones de la Policía Judicial que son llevadas a cabo en cumplimiento de un mandato judicial o de un requerimiento efectuado por el Ministerio Fiscal de aquéllas otras que se llevan a cabo por propia iniciativa o a instancia de su superior jerárquico.
>
> Respecto de las primeras resulta aplicable el artículo 11.2 d) de la Ley Orgánica 15/1999, no requiriéndose el consentimiento del interesado a la cesión, por cuanto los efectivos de la Policía Judicial solicitantes de los datos no son sino meros transmisores de la solicitud efectuada por el Ministerio Fiscal o el Órgano Jurisdiccional, actuando éste en el cumplimiento de las funciones que le han sido legalmente atribuidas y siendo el propio Juzgado o Tribunal o el Ministerio Fiscal el destinatario de los datos cedidos, como exige el artículo referido.
>
> El problema se plantea, sin embargo, en relación con aquellos supuestos en los que la Policía Judicial requiere la cesión de los datos con el fin de ejercitar las funciones de averiguación del delito y detención del

responsable, al no existir en ese caso mandamiento judicial o requerimiento del Ministerio Fiscal que dé cobertura a la cesión.

En este caso nos encontramos, a nuestro juicio, ante el ejercicio por los efectivos de la Policía Judicial de funciones que, siéndoles expresamente reconocidas por sus disposiciones reguladoras, se identifican con las atribuidas, con carácter general, a todos los miembros de las Fuerzas y Cuerpos de Seguridad del Estado.

Resultará, en consecuencia, aplicable a este segundo supuesto lo dispuesto en el artículo 22.2 de la Ley Orgánica 15/1999, según el cual "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"

Dicho informe concluía que, a juicio de esta Agencia, dicho artículo 22 venía a habilitar a los miembros de la policía judicial para la obtención y tratamiento de datos de carácter personal con las finalidades señaladas en el mismo. Dichas conclusiones resultan de aplicación al presente supuesto, en el que la legitimación para la comunicación de datos se encontrará en el ejercicio de las competencias que a la Policía municipal atribuye Ley Orgánica 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad, siempre y cuando los datos personales se recaben en la forma establecida en el artículo 22 de la Ley Orgánica 15/1999 y, tal y como a continuación se examinará, con sujeción al principio de proporcionalidad.

A ello cabe añadir que el artículo 4 de la Ley Orgánica 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad establece que "*1. Todos tienen el deber de prestar a las Fuerzas y Cuerpos de Seguridad el auxilio necesario en la investigación y persecución de los delitos en los términos previstos legalmente.*

2. Las personas y entidades que ejerzan funciones de vigilancia, seguridad o custodia referidas a personal y bienes o servicios de titularidad pública o privada tienen especial obligación de auxiliar o colaborar en todo momento con las Fuerzas y Cuerpos de Seguridad." Asimismo, el artículo 262 de la Ley de Enjuiciamiento Criminal establece que "*Los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio fiscal, al Tribunal competente, al Juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio, si se tratare de un delito flagrante."*

Cabe asimismo señalar que La Ley 5/2014, de 4 de abril, de Seguridad Privada, cuya entrada en vigor se producirá a principios del mes de junio dispone expresamente en su artículo 15.1 que "*1. 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.*

El mismo precepto en su número 2, como no podría ser de otra forma, remite a lo establecido en la Ley Orgánica 15/1999 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.*"

II

Los preceptos anteriormente citados constituyen diferentes habilitaciones legales para las diversas comunicaciones de datos a que la consulta se refiere. No obstante, debe recordarse que el derecho a la protección de datos es un derecho fundamental, tal y como ha expresado la Sentencia 292/2000 del Tribunal Constitucional, por lo que las limitaciones al mismo están sujetas al principio de proporcionalidad.

Respecto de la proporcionalidad ha señalado el Tribunal Constitucional en la Sentencia 207/1996 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)".

Cabe igualmente citar la Sentencia 17/2013 del Tribunal Constitucional, de fecha 31 de enero de 2013, por la que se resuelve el recurso de inconstitucionalidad interpuesto por el Parlamento Vasco con respecto a diversos preceptos de la Ley Orgánica 14/2003, de Reforma de la Ley orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, en la que se venía a señalar que *"Desde otro punto de vista y como ya tenemos declarado, la información que recogen y archivan las Administraciones públicas ha de ser necesaria para el ejercicio de las potestades que les atribuye la ley y adecuada a las legítimas finalidades previstas por ella (STC 254/1993, de 20 de julio, FJ 7). Así, el tratamiento de los datos por los Administraciones públicas estará subordinado a su estricta adecuación a los fines de interés público que justifican el ejercicio de las competencias correspondientes a cada una de ellas. Por ello, los datos cedidos han de ser los estrictamente necesarios para el cumplimiento de las funciones asignadas a los órganos administrativos de forma que deberá motivarse la petición de aquellos datos que resulten relevantes, pues es necesario distinguir entre el análisis y seguimiento de una situación individualizada relativa a un caso concreto y el suministro generalizado e indiscriminado de toda la información contenida en un registro personal."*

Asimismo, esta Agencia se ha pronunciado reiteradamente respecto de los requisitos que a su juicio dan cumplimiento al principio de proporcionalidad y que vienen enunciados en el informe de 14 de junio a que se hizo referencia ya continuación se transcriben:

"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".

Teniendo en cuenta todo lo anteriormente señalado respecto de la aplicación del principio de proporcionalidad, debe examinarse si los diferentes accesos a los datos a que hace referencia la consulta responden a dicho principio.

No se examina aquí la proporcionalidad de los accesos en tiempo real a las imágenes ni la entrega de las grabaciones cuando se efectúen en virtud de requerimiento efectuado por el Ministerio Fiscal o de mandamiento judicial, ya que dichos supuestos, como se ha señalado, se incardinan en la habilitación para la cesión de datos prevista en el artículo 11.2. d) de la Ley Orgánica 15/1999, y ambos instrumentos vendrían a determinar los parámetros a que deben ajustarse tales accesos para que resulten conformes al principio de proporcionalidad.

En lo que respecta a los demás supuestos, el primero de ellos, relativo al acceso en tiempo real a las imágenes de las cámaras captadas por el consultante cuando el conductor acciona el dispositivo de emergencias, parece resultar ajustado a los requisitos señalados en los informes de esta Agencia para concretar dicho principio 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. En el caso a que se hace referencia aquí, dicha petición viene concretada al momento en que la intervención policial se solicita por la propia entidad consultante por estarse produciendo una situación de riesgo para la seguridad o la efectiva comisión de un delito, por lo que la visualización de las imágenes de los hechos que motivan la solicitud de intervención por la policía, para determinar las actuaciones a seguir en dicho caso, reuniría los requisitos mencionados para considerarse conforme al principio de proporcionalidad.

En lo que respecta a la puesta a disposición de la policía municipal de las grabaciones efectuadas por las cámaras de la entidad consultante, relacionadas con la comisión de un delito que haya sido objeto de denuncia por un ciudadano, la comunicación de las imágenes en que se constate la comisión del delito, efectuada tras una petición individualizada y motivada por parte de la policía, será conforme a dicho principio. De la misma manera, en aquellos supuestos en que el consultante constate 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 será igualmente conforme al principio de proporcionalidad.

Más difícil resulta determinar la proporcionalidad del acceso los accesos en los demás supuestos, en los que la visualización tiene como objetivo, no la comprobación de la existencia de un delito ya cometido o que se está produciendo, sino su posible prevención. En este sentido, 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.

III

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.