

Informe jurídico 0193/2007

### **Ejercicio de derechos en Videovigilancia**

La consulta plantea, varias cuestiones relativas a la Instrucción 1/2006, de 8 de noviembre de 2006, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

En primer lugar se plantea, por parte de la entidad consultante la carencia de herramientas que permitan acceder de forma automática a las imágenes. En este sentido, sólo podemos indicar que la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, no exige ningún sistema concreto para el reconocimiento de las imágenes como datos de carácter personal, quedando por tanto, la elección del sistema al arbitrio de la consultante.

Este criterio es el que ha mantenido el Tribunal Constitucional que en relación con la actuación de Administración Pública permite deducir que quien trata los datos, es responsable de cumplir con todo aquello que la legislación determina, así lo establece en su Sentencia 254/1994 fundamento jurídico “3. *Tampoco resultan convincentes las afirmaciones que realiza acerca de la imposibilidad material en que se encontraban las autoridades a las que el Sr. X. dirigió su instancia para contestar a sus peticiones de información. El que un determinado órgano administrativo disponga, o carezca, de los medios materiales o de las atribuciones competenciales precisos no sirve para discernir los derechos de un ciudadano, especialmente si esos derechos son declarados por la Constitución. La cuestión que debemos determinar en este proceso es si el actor tenía o no derecho, en virtud del art. 18 C.E., a que la Administración le suministrase la información que solicitaba. Si tiene derecho a ella, es deber de todos los poderes públicos poner los medios organizativos y materiales necesarios para procurársela; si no tiene derecho, sigue siendo igualmente irrelevante el que dichos medios existan o no*”

En segundo lugar la consultante plantea, si realmente existe tratamiento de datos personales cuando las imágenes, no vayan a poder identificar a una concreta



persona. Sobre este punto se ha pronunciado la Agencia Española de Protección de Datos en diversos informes, pudiendo destacarse el de fecha de 20 de diciembre de 2006 que señala lo siguiente:

*“Por ello, la grabación de la imagen de una persona ya sea trabajador o no de la empresa, es un dato personal, siendo éste el criterio de la Agencia Española de Protección de Datos, tal y como se ha señalado en la Resolución R/00035/2006 de 27 de febrero de 2006, donde se establece que:*

*“El artículo 1 de la LOPD dispone: “La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”.*

*En cuanto al ámbito de aplicación de la citada norma, el artículo 2.1 de la misma señala: “La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”; definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como “Cualquier información concerniente a personas físicas identificadas o identificables”.*

*El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas “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”. La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.*



*De acuerdo con aquella definición de tratamiento de datos personales, la captación de imágenes de las personas que transitan una vía pública constituye un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada.*

*El artículo 1.4 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continúa en vigor de conformidad con lo establecido en la disposición transitoria tercera de la LOPD, considera datos de carácter personal a “toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable”.*

*En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE del Parlamento 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, según el cual, a efectos de dicha Directiva, se entiende por dato personal “toda información sobre una persona física identificada o identificable; 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, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para 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 aquélla.*

*Atendiendo a la definición contenida en las normas citadas, que considera dato de carácter personal “cualquier información concerniente a personas físicas identificadas o identificables”, las*



*grabaciones indicadas se ajustarán a este concepto siempre que permitan la identificación de las personas que aparecen en dichas imágenes. La Directiva 95/46/CE en su Considerando 14 lo afirma expresamente al señalar:*

*“(14)Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;”.*

#### IV

*El Grupo de protección de las personas, en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la citada Directiva 95/46/CE, en su Dictamen 4/2004, adoptado en fecha 11/02/2004, relativo al tratamiento de datos personales mediante vigilancia por videocámara, formula distintos criterios para evaluar la legalidad y conveniencia de instalar sistemas de captación de imágenes en zonas públicas. En relación al tratamiento de datos constituidos por imagen y sonido relativos a personas físicas, en dicho documento se declara la plena aplicabilidad de las disposiciones de la citada Directiva relativas a:*

*. Calidad de los datos: Las imágenes serán tratadas de manera leal y lícita, y se destinarán a fines determinados, explícitos y legítimos. Se utilizarán de conformidad con el principio según el cual los datos deberán ser adecuados, pertinentes y no excesivos, y no serán tratados posteriormente de manera incompatible con dichos fines; se conservarán durante un periodo limitado, etc.*

*. Principios relativos a la legitimación del tratamiento de datos: En base a estos principios, es necesario que el tratamiento de datos personales mediante vigilancia por videocámara esté fundamentado en al menos uno de los requisitos mencionados en el artículo 7 (consentimiento inequívoco, necesidad de obligaciones contractuales,*



*de cumplimiento de una obligación jurídica, de protección de un interés vital del interesado, de cumplimiento de una misión de interés público o inherente al ejercicio del poder público, equilibrio de intereses, etc.).*

*. Tratamiento de categorías especiales de datos, sujeto a las garantías aplicables al uso de datos sensibles o datos relativos a infracciones en el marco de la vigilancia por videocámara (con arreglo al artículo 8).*

*. Información que se facilitará al interesado (artículos 10 y 11).*

*. Derechos del interesado, en concreto el derecho de acceso y el derecho de oposición al tratamiento por razones legítimas (artículo 12 y letra a) del artículo 14).*

*. Garantías aplicables en relación con las decisiones individuales automatizadas (artículo 15).*

*. Seguridad de las operaciones de tratamiento (artículo 17).*

*. Notificación de las operaciones de tratamiento (artículos 18 y 19).*

*. Controles previos de las operaciones de tratamiento que puedan presentar riesgos específicos para los derechos y libertades del interesado (artículo 20).*

*. Transferencia de datos a terceros países (artículo 25 y siguientes).*

*Por otra parte, para determinar si el supuesto que se analiza implican el tratamiento de datos relacionados con personas identificables, el citado Grupo considera que los datos constituidos por imagen y sonido son personales aunque las imágenes se utilicen en el marco de un sistema de circuito cerrado y no estén asociados a los datos personales del interesado, incluso, si no se refieren a personas cuyos rostros hayan sido filmados, e independientemente del método utilizado para el tratamiento, la técnica, el tipo de equipo, las características de la captación de imágenes y las herramientas de comunicación utilizadas. A efectos de la Directiva, se añade, el carácter identificable también puede resultar de la combinación de los datos con información procedente de terceras partes o, incluso, de la*



*aplicación, en el caso individual, de técnicas o dispositivos específicos.*

*En cuanto a las obligaciones y precauciones que deberán respetarse por los responsables del tratamiento de los datos se mencionan, entre otras, la de evitar las referencias inadecuadas a la intimidad; especificar de forma clara e inequívoca los fines perseguidos con el tratamiento y otras características de la política de privacidad (momento en que se borran las imágenes, peticiones de acceso); obtención del consentimiento del interesado basado en una información clara; mantener la necesaria proporcionalidad entre los datos y el fin perseguido, obligándose al empleo de sistemas idóneos con respecto a dicho fin y a minimizar los datos por parte del responsable del tratamiento; datos que han de ser adecuados, pertinentes y no excesivos y deberán retenerse durante un plazo en consonancia con las características específicas de cada caso....*

*Por tanto, la captación y grabación de imágenes con fines de vigilancia y control, como es el caso que nos ocupa, se encuentra plenamente sometida a lo dispuesto en la LOPD, máxime cuando los afectados resultan perfectamente identificables, dentro del ámbito donde se realiza la captación de imágenes(...).*

*Además este es el criterio que se hace constar en la Instrucción 1/2006 de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, que se publicó en el B.O.E de 12 de diciembre de 2006, pues así lo dispone su artículo uno en el que se señala que “La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.*

*El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento*



*de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.*

*Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.”*

## II

A continuación, plantea la consultante si la Instrucción 1/2006, ha modificado en algún punto el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. La respuesta es clara, la Instrucción no ha modificado en ningún punto la regulación que de los derechos se efectúa en la Ley Orgánica 15/1999. EL principio de jerarquía normativa impide que una Instrucción modifique el contenido dispositivo que se encuentra en una norma de rango legal.

En cuanto al modo de ejercitar los derechos de acceso, rectificación, cancelación y oposición de los afectados, cualquier afectado podrá ejercitar sus derechos ante el responsable del fichero y éste deberá en todo caso atenderlos y responderlos, dado que así lo indica lo dispuesto en la norma segunda punto tercero de la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, donde se señala que “El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud.(.....). En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.”

En conclusión, el responsable del fichero deberá de atender las peticiones de los ciudadanos y deberá de responderlas , pues en caso de no atender la petición de ejercicio de los derechos, el ciudadano podrá al amparo del artículo 18 de la Ley Orgánica 15/1999 y que se reproduce en la Instrucción recabar la tutela por parte de la Agencia.

Asimismo el acceso que se efectúe no puede implicar una violación a los derechos de terceros, por tanto el sistema que prevé la Instrucción en su artículo 5 que transcribimos “2. - El responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.” ,asegura el equilibrio entre ambos derechos, esto es atender el acceso y no comunicar datos de terceros. No obstante, la consultante podrá adoptar de otros medios iguales de efectivos, siempre que dicho equilibrio se mantenga.

### III

En tercer lugar se plantea la forma de ejercicio del derecho de cancelación de las imágenes. Respecto de la forma del ejercicio del derecho de cancelación, la Ley orgánica 15/1999, en el artículo 16 de la Ley Orgánica 15/1999 dispone que, “el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de cancelación del interesado en el plazo de diez días”, estableciendo su apartado 2 que “serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos”. En consecuencia, para que se proceda a la cancelación de las imágenes, el afectado debería de acreditar que sus datos resultan inexactos o incompletos, cuestiones que resultan difícil de acreditar en las imágenes. No obstante, si un particular solicita la cancelación de sus imágenes, el responsable del fichero debería de cancelar las imágenes en el plazo de 10 días desde que se produce la solicitud. Sin embargo, sí las grabaciones son canceladas cada 24 horas, implicaría que los datos de carácter personal del solicitante han resultado ya cancelados, y el responsable del fichero deberá de informar al afectado que sus datos ya han sido cancelados.

Respecto al plazo, sobre el que han de conservarse las imágenes, la elección de dicho plazo, no es arbitraria y sino que encuentra su fundamento tanto en la Instrucción 1/1996, sobre ficheros automatizados establecidos con la finalidad de acceder de controlar el acceso a los edificios, que en su norma quinta prescribe que “Los datos de carácter personal deberán ser destruidos cuando haya

transcurrido el plazo de un mes, contado a partir del momento en que fueron recabados”. Y a mayor abundamiento se ha tenido en cuenta el criterio utilizado por el legislador en la regulación de las Fuerzas y Cuerpos de Seguridad del Estado, aunque se refiera a un concreto ámbito específico de aplicación.

Por último se plantea, cómo ha de actuarse en el caso de que una persona solicite el ejercicio del derecho de cancelación y al tiempo se conozca la existencia de una incidencia de seguridad.

En primer lugar, al no concretar que se entiende por incidencia de seguridad, no podemos otorgar una solución clara al respecto, pues puede afectar a cuestiones de seguridad pública o por el contrario a fallos en el sistema informático. La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal viene a señalar que la cancelación dará lugar al bloqueo de los datos de carácter personal en su artículo 16.3, 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”.

Este precepto, a su vez, se complementa con la previsión contenida en el transcrito artículo 16.5 de la Ley Orgánica 15/1999. En relación con esta cuestión, ya se indicaba en nuestros informes de 30 de julio de 2004 y 1 de agosto de 2005 lo siguiente:

*“(...) la Ley Orgánica 15/1999 viene regular el bloqueo de los datos de carácter personal en su artículo 16.3, 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”.*

*Este precepto, a su vez, se complementa con la previsión contenida en el artículo 16.5 que indica que “los datos de carácter personal*



*deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado”.*

*Del análisis conjunto de las normas citadas se desprende que existirán supuestos en los que si bien deberá procederse a la cancelación de los datos, al haber dejado de ser necesarios para la finalidad que justificó su tratamiento, como sucederá cuando se haya producido la completa consumación del contrato que vincula al responsable del tratamiento con sus clientes, dicha cancelación deberá producirse mediante el bloqueo de los datos de carácter personal sometidos a tratamiento que, produciendo unos efectos similares al borrado físico de los datos, salvo en determinadas circunstancias, descritas por el artículo 16.3 de la Ley Orgánica, no implicará automáticamente ese borrado.*

*Así, el artículo 16.3 viene a reconocer, en consonancia con lo previsto en el artículo 16.5 de la Ley, que existirán determinados supuestos en los que la propia relación jurídica que vincula al afectado con el responsable del fichero y que determina, en definitiva, el tratamiento del dato de carácter personal cuya cancelación se pretende, así como las obligaciones de toda índole que pudieran derivarse de la citada relación jurídica y que aparecen impuestas por la Ley, impedirá que la cancelación se materialice de forma inmediata en un borrado físico de los datos.*

*Por el contrario, el responsable del fichero estará obligado, bien por el contenido de aquella relación jurídica, bien por lo establecido en una norma imperativa, al mantenimiento del dato, si bien sometido a determinadas condiciones que aseguren y garanticen el derecho del afectado a la protección de sus datos de carácter personal, no pudiendo disponer de tales datos en la misma medida en que podría hacerlo en caso de que no procediera (de oficio –por haber dejado de*



*ser necesarios para el cumplimiento de la finalidad del fichero- o a solicitud del afectado) la cancelación de los mismos.*

*En cuanto a las causas que podrán motivar la conservación del dato, sujeto a su previo bloqueo, y al margen de la relación jurídica con el afectado, a la que se refiere el artículo 16.5 de la Ley Orgánica 15/1999, éstas deberán fundarse en lo dispuesto “en las disposiciones aplicables” o a la “atención de las posibles responsabilidades nacidas del tratamiento”, tal y como prevé la meritada Ley.*

*En este sentido, para la determinación del período de bloqueo de los datos debe tenerse en cuenta que la Sentencia del tribunal Constitucional 292/2000, de 30 de noviembre, viene a imponer, expresamente, el principio de reserva de Ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho (como sería la derivada del artículo 16.3 de la Ley) deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado. Así, a título de ejemplo, podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento, en los términos previstos por la legislación civil o mercantil que resulte de aplicación, así como el plazo de cuatro años de prescripción de las deudas tributarias, en cuanto los datos puedan revestir trascendencia desde el punto de vista tributario (habida cuenta de la obligación de conservación que impone el artículo 111 de la Ley General Tributarias y el plazo legal de prescripción de cuatro años previsto en el artículo 24 de la Ley de Derechos y Garantías de los Contribuyentes).*

*En todo caso, debe recordarse que el mantenimiento del dato bloqueado, supone una excepción al borrado físico del mismo que, en definitiva, es el fin último de la cancelación (tal y como prevé el propio artículo 16.3, al indicar que “cumplido el citado plazo deberá procederse a la supresión).*



*En consecuencia, a nuestro juicio, la cancelación no supone automáticamente en todo caso un borrado o supresión físico de los datos, sino que puede determinar, en caso de que así lo establezca una norma con rango de Ley o se desprenda de la propia relación jurídica que vincula al responsable del fichero con el afectado (y que motiva el propio tratamiento), el bloqueo de los datos sometidos a tratamiento.*

*En lo atinente a la determinación de los períodos en que el dato habrá de permanecer bloqueado, en relación con lo dispuesto en el artículo 16.3, resulta imposible establecer una enumeración taxativa de los mismos, debiendo, fundamentalmente, tenerse en cuenta, como ya se ha indicado con anterioridad, los plazos de prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula al consultante con su cliente, así como los derivados de la normativa tributaria o el plazo de prescripción de tres años, previsto en el artículo 47.1 de la propia Ley Orgánica 15/1999 en relación con las conductas constitutivas de infracción muy grave.*

*Por último, en cuanto al modo de llevar a cabo el bloqueo, deberá efectuarse de forma tal que no sea posible el acceso a los datos por parte del personal que tuviera habitualmente tal acceso, por ejemplo, el personal que preste sus servicios en el centro consultante, limitándose el acceso a una persona con la máxima responsabilidad y en virtud de la existencia de una requerimiento judicial o administrativo a tal efecto. De este modo, pese a permanecer el tratamiento de los datos, el acceso a los mismos quedaría enteramente restringido a las personas a las que se ha hecho referencia.”*

En consecuencia, la consultante deberá proceder a la cancelación y bloqueo de los datos de los afectados, durante los plazos establecidos por la legislación especial en la materia debiendo, en cuanto a los restantes supuestos, dar

cumplimiento íntegro a las obligaciones previstas en la Ley Orgánica 15/1999, de 13 de diciembre.

#### IV

En cuarto lugar se plantean dudas relativas al ejercicio del derecho de oposición .En cuanto al derecho de oposición, el artículo 6.4 de la Ley Orgánica dispone que “En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado”.

Por tanto el ejercicio del derecho de oposición en los casos en los que no sea necesario el consentimiento requiere la concurrencia de los requisitos exigidos en el artículo 6.4 antes expuesto.

En primer lugar es necesario que se alegue un motivo fundado y legítimo, relativos a la situación personal de cada afectado, para poder valorar si procede o no, por tanto al desconocer los supuestos en los que se plantea la oposición, no podemos otorgar una solución concreta.

#### IV

Por último respecto al modo de ejercicio del derecho de rectificación, dispone la Instrucción 1/1998, en su Norma tercera, apartado tercero que “La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que deba de realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado.” Por tanto en el supuesto planteado, al ser la imagen el dato personal, el afectado no podrá indicar que el dato es erróneo, dado que nuestra imagen es la que es, lo que no es óbice para que el responsable del fichero, deba atender la solicitud del afectado y contestarla en el plazo de cinco días que así establece el apartado segundo de la Norma tercera de la mencionada Instrucción que señala “Los derechos de rectificación y cancelación se harán



efectivos por el responsable del fichero dentro de los cinco días siguientes a la recepción de la solicitud”