Nuevas tecnologías, videovigilancia, derecho a la protección de datos y ficheros policiales[1]

IGNACIO VILLAVERDE MENÉNDEZ

Profesor titular de Derecho constitucional
Secretario general de la Universidad de Oviedo

1. UNAS CONSIDERACIONES GENERALES

Conviene iniciar estas reflexiones recordando que la protección de datos no se reduce exclusivamente al ámbito de aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal (en adelante, LOPD). El Tribunal Constitucional (en adelante, TC) ha declarado en su Sentencia 292/2000 que la protección de los datos personales es un derecho fundamental que deriva del art. 18.4 de la Constitución Española de 1978 (en adelante, CE). Como tal, si se me permite la expresión, tiene una vida propia al margen de la LOPD, limitándose ésta a desarrollar el derecho, y a regular su ejercicio en alguno de sus extremos, en aquellos ámbitos que resultan de lo dispuesto en sus arts. 2 y 3; pero que no agota el ámbito de aplicación del derecho fundamental a la protección de los datos personales. Adviértase, además, que la aplicación de la LOPD, además, está condicionada a que el datos personal sea objeto de registro «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» (art. 2.1 LOPD); considerándose «tratamiento» a 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» (art. 3. c) LOPD). La forma más gráfica de explicar esto es que, después de las SSTC 290 y la STC 292/2000, sería indiferente que existiese o no la LOPD o una norma regulado-

1. Este texto es la transcripción revisada de la intervención de su autor en el Curso cuyas ponencias constituyen el contenido de este libro. Aprovecho estas líneas para agradecer al profesor Vicenç Aguado, y a la Escola de Policia de Catalunya, en la persona de su Director, don Joan Mauri i Majós, su amable y generosa invitación para que participara en este prestigioso Curso sobre seguridad Pública y privada.

ra de la protección de datos. La razón de ello es que la protección de datos ya es un derecho fundamental dotado de eficacia directa con un contenido constitucional definido en estas Sentencias y que, además, es de aplicación general (ámbito objetivo) y universal (ámbito subjetivo). En lo relativo al derecho fundamental, por tanto, no hay excepciones de aplicación, como sí las hay en cambio en la aplicación de la LOPD. Es importante no perder de vista esta proposición para entender cabalmente algunas de las cuestiones que se abordarán en las páginas que siguen.

Otro apunte que su importancia tendrá en estas páginas es el referido a los fines constitucionalmente legítimos de la actuación de las Fuerzas y Cuerpos de Seguridad del Estado, de las Comunidades Autónomas donde las haya y de los entes locales (en adelante, FFCCSS). Este apunte está ligado, evidentemente, a los dos últimos puntos de este opúsculo donde se describe la interactuación de la protección de datos y la interceptación de las telecomunicaciones y la videovigilancia. El enfoque de estas páginas será siempre el de la perspectiva de las obligaciones que a las FFCCSS impone la garantía del derecho fundamental a la protección de los datos personales y las que resultan del desarrollo de este derecho fundamental por la LOPD.

Las tesis que se tratará de sostener aquí son, en primer lugar que el cambio de objeto o de medio o de técnica, el que ya no se hable de correo postal o de «teléfono» sino que de correo electrónico o de «móviles» de última generación o de medios telemáticos o electrónicos de comunicación, no cambia para nada el sistema de garantías constitucionales en materia de interceptación de las comunicaciones. El contenido del derecho fundamental al secreto de las comunicaciones del art. 18.3 CE sigue siendo el mismo sea cual sea el medio empleado para comunicarse o para interceptar la comunicación. Por tanto, el art. 579 LECrim sigue siendo de aplicación estemos hablando de una carta o estemos hablando de un correo electrónico o estemos hablando de una llamada a un teléfono fijo o bien una comunicación electrónica a través de un SMS, etc. Los avances de la tecnología no suponen, a nuestro juicio, ningún cambio en la estructura ni en el contenido de las garantías constitucionales relativas al secreto de las comunicaciones o a la protección de datos.

En segundo lugar, y como ya se dijo, el régimen jurídico de la protección de datos no se limita a lo dispuesto en la LOPD. Así por ejemplo, aunque la LOPD excluye de su ámbito de aplicación «a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada» (art. 2.2.c), no por ello las investigaciones policiales en materia de terrorismo o de la actividad delictiva organizada son un espacio inmune exento de las garantías constitucionales de la protección de datos.

En tercer lugar, cabe distinguir la actividad de prevención ligada a la garantía de la seguridad pública, de encaje constitucional en el art. 104 CE, de la actividad represiva del delito; es decir, entre la *policía administrativa de seguridad* donde la actuación de las FFCCSS van dirigidas a un fin muy específico como es el de la prevención del daño en bienes y personas, y la *policía judicial*, que se mueve en un plano distinto, el cual es el de la lucha procesal y judicial contra la delincuencia. Son planos distintos constitucionalmente, y responden a esquemas y estructuras de

garantías también distintas. El Legislador consciente o inconscientemente ha tenido presente esta distinción. Prueba de ello es que cuando la Ley Orgánica 4/1997, de 4 de agosto, reguladora de la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado de Videovigilancia (en adelante, LOV), norma la instalación de las video-cámaras fijas, o hace lo propio para el uso de video-cámaras móviles, lo hace a los efectos del ejercicio de las funciones propias de la *policía administrativa*. En cambio, cuando los FFCCSS actúan en su condición de *policía judicial*, el marco de su actuación en materia de videovigilancia no es la LOV, debiendo remitirse su régimen a la LECrim y no la LOV.

Bien se ve que el contexto normativo resulta bastante complejo y denso. Trataremos de agruparlo en tres grandes sectores. Uno relativo a la *policía administrativa de seguridad*, otro al de *policía judicial* y finalmente otro ámbito que suele eludirse, pero que es de enorme importancia, cual es el referido a la actuación de los servicios secretos, en el caso español del Centro Nacional de Inteligencia (CNI).

Cualquiera de las actividades que van a ser objeto de estudio en este trabajo suponen recabar y tratar datos de carácter personal, sea en soporte digital, sea cual sea el soporte empleado. Recuérdese que dato personal es cualquier información concerniente a personas físicas identificadas o identificables (art. 3.a) LOPD, y que la STC 292/2000 elevó a definición del objeto del derecho fundamental a la protección de los datos personales), lo que se extiende también a las imágenes de las personas, siempre que permita su identificación.[2] No hay que olvidar que el derecho fundamental a la protección de los datos personales y la propia LOPD se aplica a cualquier tipo de medio que soporte el dato personal (analógico

2. *Mutatis mutandis*, merece la pena transcribir aquí el siguiente Informe de la Agencia española de Protección de Datos sobre videovigilancia en el lugar de trabajo (Año 2001): «Se planteó si resulta conforme a lo establecido en la LOPD la instalación de cámaras para el control de la actividad de los trabajadores de la entidad consultante. La primera cuestión a resolver fue discernir si las imágenes y sonidos que se obtendrían por tales sistemas de registro se encontraban sometidas a lo dispuesto en la mencionada Ley Orgánica. Para ello fue necesario efectuar dos acotaciones previas: *a*) En primer lugar, se plantea el problema de si dichas imágenes y sonidos pueden ser consideradas como datos de carácter personal, de conformidad a lo establecido en la Ley Orgánica de 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal. A tal efecto, y con carácter general, debe indicarse que los artículos 1 y 2 de la citada Ley, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento automatizado de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la Ley Orgánica como "cualquier información concerniente a personas físicas identificadas o identificables". *b*) En segundo término, y aun cuando nos hallemos ante un supuesto en que existan datos de carácter personal, será necesario que dichos datos se encuentren incorporados a un fichero, definido como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso", por el artículo 3 b) de la Ley. Pues bien, en relación con el primero de los criterios a los que se ha hecho referencia, debe indicarse que las imágenes a las que se refiere la consulta sólo podrán ser consideradas datos de carácter personal en caso de que las mismas permitan la identificación de las personas que aparecen en dichas imágenes, no encontrándose amparadas en la Ley Orgánica en caso contrario. Así, en supuestos en que las imágenes se tomaran del lugar de trabajo sí se produciría dicha identificación, dado que siempre aparecerían en las mismas los trabajadores de la empresa en su lugar de actividad (lo que les hace perfectamente identificables)». Puede consultarse en www.agpd.es, en las secciones «Canal de documentación», «Informes», «Otras cuestiones de interés».

o digital). Pero no cabe duda que la interceptación de comunicaciones o la grabación de imágenes y sonidos también afecta a muchos otros derechos fundamentales (en ocasiones, alcanzan también a la libertad de expresión e información o al derecho al honor).[3] Ante todo, nos interesa, fundamentalmente, estos cuatro derechos fundamentales: protección de datos, secreto de las comunicaciones, derecho a la propia imagen y derecho a la intimidad. Y a ellos nos ceñiremos.

2. El contenido constitucional de la protección de datos

El derecho fundamental a la protección de datos personales es, indudablemente, el más novedoso de las mencionadas líneas más arriba; acaso por ello convenga detenerse un instante en la definición de su contenido.

Ese contenido constitucional del derecho fundamental a la protección de los datos personales se concreta en una serie de puntos muy simples pero capitales. En primer lugar, la protección de datos no es una garantía del secreto del dato sino de ciertas condiciones para su legítimo uso por terceros distintos al afectado. Cuando el TC trata de distinguir la protección de datos del derecho a la intimidad precisamente se centra en que primero el objeto de la protección de datos no es un dato íntimo sino, precisamente, un dato revelado (STC 292/2000). Lo que trata de proteger el derecho fundamental de la protección de datos no es la opacidad del dato, ni su *intimidad* o el control sobre quien puede conocer un dato relativo a la vida personal o familiar. Justamente el objeto de protección del derecho fundamental es el dato ya conocido, bien porque se ha consentido su conocimiento por terceros, o bien porque una norma así lo dispone. El dato ha salido de la esfera privada del sujeto, y se trata ahora de establecer en qué condiciones su tráfico, su circulación es constitucionalmente adecuada.

El objeto del derecho fundamental de la protección de datos es, por tanto, el régimen de conocimiento, uso y destino de un dato que ha salido del ámbito de la vida privada, personal y familiar, de la persona. Este es el objeto del derecho fundamental a los datos que dota a su titular de un poder jurídico de disposición sobre la publicidad del dato personal (STC 292/2000). Esta es la clave de bóveda del régimen constitucional y legal de la protección de datos: el pleno control de la persona sobre el uso y destino de sus datos personales. De ahí derivan los principios de consentimiento informado y finalidad que cierran el sistema: salvo excepción legal, sólo se pueden hacer uso de los datos de una persona si esta ha consentido

3. El tema de las telecomunicaciones se ha puesto de especial relieve en la actualidad diaria como resultado del anuncio por parte de las autoridades de la Unión Europea, que ha sido coreado con una cierta imprudencia por parte de nuestro Ministro del Interior, respecto de la interceptación, uso y tratamiento de los datos que él llama objetivos de las comunicaciones entre particulares. Se considera que el dato objetivo de quien está conversando, desde donde y a través de que medio lo hace no afecta al secreto de las comunicaciones. Esto es un error por cuanto la jurisprudencia del TEDH y del TC han afirmado de forma reiterada que el conocimiento de esos datos objetivos también hay que integrarlo dentro del campo de garantías del artículo 18.3 de la Constitución.

y lo ha hecho con pleno conocimiento de los datos que serán usado y con qué finalidad, así como de los derechos que le asisten (acceso, rectificación, cancelación y oposición), asimismo el uso d elos datos estará sometido siempre a un fin conocido por el interesado, explícito, inequívoco, determinado y legítimo.

Así lo ha expresado la STC 292/2000:

> De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.
>
> En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele (FJ 7).
>
> De manera que, privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo estará también de su derecho fundamental a la protección de datos, puesto que, como concluyó en este punto la STC 11/1981, de 8 de abril (FJ 8), se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección (FJ 10).

El TC ha aseverado rotundo como contenido esencial de este derecho fundamental el derecho de información del interesado. Evidentemente, el individuo no puede controlar qué se hace con sus datos si no sabe que su dato lo tiene un tercero y lo puede usar. Por lo tanto, es capital para la efectiva garantía y respeto del derecho tener informado al afectado de quién tiene sus datos, para qué y con qué finalidad, a efectos de conocer el posible destino que pueden darse a sus datos personales. Además, ese conocimiento permite al afectado poder reaccionar fren-

te a la obtención y uso de sus datos ejerciendo los derechos de oposición al tratamiento y de rectificación y cancelación de los datos.

La STC 292/2000 (FJ-13) subraya que:

> De suerte que, sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia.

Este contenido esencial del derecho fundamental tiene eficacia directa. Es decir, se aplica directamente a cualquier relación o situación jurídica en la que se empleen datos personales. Da igual que sea la captación por una cámara de la imagen o del sonido de un individuo; en ambos casos ya hemos visto que se trata de de *datos personales* porque permiten la identificación de la persona. Por tanto, es indiferente que sea la grabación de una conversación o el conocimiento del listado de llamadas hechas o recibidas desde un teléfono móvil o la grabación o toma de imágenes de una persona o personas, todo esto son datos personales y están sujetos a ese conjunto de garantías que componen el contenido esencial del derecho fundamental a la protección de datos que ha definido el TC, en especial en su Sentencia 292/2000.

3. Las líneas maestras de la protección de datos. Calidad de los datos y principios generales de su protección

Ese contenido constitucional se ha desarrollado por la LOPD, y también por la Directiva comunitaria 95/46/CE, fijando, de un lado, la «calidad de los datos» y los principios generales que han de regir su garantía y respeto.

El artículo 4 LOPD, transponiendo la Directiva 95/46/CE, fija los criterios que definen la «calidad» de los datos, o, para ser más exactos, el estándar lícito del tratamiento de los datos personales. En lo que ahora nos interesa, los datos personales consistentes en imágenes o en informaciones digitales «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». No cabe emplear los datos «para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos», con la excepción de tratamientos con fines históricos, estadísticos o científicos. Conviene en esto recordar que la jurisprudencia de la Audiencia Nacional ha variado de forma sustancial el entendimiento de qué deba considerarse un fin incompatible. A su juicio, sólo cabe compatibilidad entre fines similares. Así pues, se vuelve al criterio originario de la legislación anterior a la LOPD en la que, como ahora por obra de la Audiencia Nacional, no caben tratamientos de datos para fines distintos, aunque sean compatibles, con los originariamente expresados al tiempo del recabamiento de los datos.

El precepto fija también los siguientes principios, que literalmente se transcriben del precepto citado:

1. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
2. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados.
3. 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.
4. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
5. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

La LOV en su artículo 6 establece los «principios de utilización de las videocámaras» que en buena medida se compadecen con los criterios de «calidad de los datos» antes descrito y que, complementados por estos últimos, darían cobertura sobrada al uso de sistemas de videovigilancia desde la perspectiva del derecho fundamental a la protección de los datos personales.[4]

No cabe duda de que el *principio de finalidad* es la clave de bóveda del sistema. La identificación precisa y conocida de los propósitos perseguidos en el tratamiento de los datos personales, también de las imágenes que permitan identificar a la persona o de sus comunicaciones electrónicas, es el anclaje al que se unen los principios de información y consentimiento, de los que se hablará más abajo, y que constituyen las tres líneas maestras del régimen de la protección de los datos personales. Tanto para las Agencias, estatal y autonómicas, de protección de datos como para la jurisprudencia se vulnera el derecho a la protección de datos si no se le deja muy claro al afectado para que se quieren esos datos y si no se

4. *Principios de utilización de las videocámaras.* 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».

dice con cierto grado de precisión o de concreción. El rechazo al empleo de finalidad genéricas, impide acudir a los «fines constitucionalmente legítimos» de la actividad de la FFCCSS para justificar así el tratamientos de datos personales. No basta por tanto con la cita genérica del artículo 104 CE (proteger el libre ejercicio de los derechos y libertades y la seguridad ciudadana). Se tiene que precisar que motivo o finalidad concreta se está persiguiendo con esa actividad policial en la que se están recabando datos personales. No se puede justificar sin más la captación de imágenes de una persona alegando razones de seguridad pública o de defensa nacional o la prevención y persecución de los delitos. Todo ello va ligado a la idea de inequívoco. Es decir, no caben ambigüedades en la definición de las finalidades. Las finalidades tienen que estar muy claras. Ello de tal manera que el afectado entienda perfectamente y sea consciente de la finalidad a la que van a dedicar los datos que se le piden o que ya se han obtenido.

Por otra parte, y prueba de la importancia del principio de finalidad y su estricta observancia, el uso y cesión de los datos para el mismo tipo de fin exige únicamente el consentimiento inicial manifestado al tiempo de su recogida. Este consentimiento prestado para el uso de los datos con un fin determinado y explícito se extiende también a usos posteriores de los datos, incluso los derivados de cesiones a terceros, siempre que esos usos persigan un fin similar (esto es, que no sea distinto) al que justificó su recogida y del que fue informado el afectado en ese momento.[5]

Mayores cuestiones suscita el uso de esos datos para fines distintos, pero compatibles, con los que justificaron su recogida. En este caso, la compatibilidad de fines haría lícita la cesión de los datos, según dispone el artículo 11.2 LOPD, pero exige un nuevo y específico consentimiento sobre la nueva finalidad perseguida con el uso de los datos. Desde luego, la LOPD veda el uso de los datos personales para fines distintos a los que motivaron su recogida, exigiendo, de pretender usarlos de ese modo, la puesta en conocimiento al interesado del nuevo destino de sus datos y el recabamiento de su consentimiento para que así sea. La STC 292/2000 ha sido meridiana en este extremo: «... la cesión de los mismos (los datos se refiere) a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando sean compatibles con éstos (art 4.2), supone una nueva posesión y uso que requiere el consentimiento del interesado».

Es cierto que la LOPD habla de fines «incompatibles», lo que inicialmente fue entendido como la autorización legal para que los datos se destinaran a fines distintos de los que alentaron su recogida sin que fuese necesario un nuevo consentimiento del afectado siempre que esos fines fueran compatibles con los del recabamiento de los datos. Sin embargo, las Sentencias de la Audiencia Nacional, Sala de lo Contencioso Administrativo, de 8 de febrero de 2002 y 11 de diciembre de 2004, con apoyo en la STC 292/2000, han afirmado que a pesar de la dicción literal del artículo 4 LOPD, los fines de recogida y de cesión deben ser similares, no basta

5. De hecho la Agencia de Protección de Datos considera que el consentimiento a un tratamiento para un fin determinado se extiende tácitamente a las cesiones que persigan idéntica finalidad.

con su compatibilidad, para entender que el consentimiento dado por el afectado para que sus datos fuesen recogidos para un fin también se extiende a las cesiones que de ellos se haga a terceros.

Conviene reparar también en que la Sentencia del Tribunal Supremo, Sala Tercera, de 15 de abril de 2002 afirma, en aplicación de la STC 292/2000, que la cesión o comunicación de datos entre Administraciones públicas para precisamente alcanzar el fin o uno de los fines a los que obedeció la recogida del dato, no requiere reiterar el consentimiento prestado al tiempo de su recogida. En esta líneas, la Agencia de Protección de Datos ha mantenido en sus Resoluciones que, existiendo identidad de fines entre los comunicados al interesado para recabar sus datos y los perseguidos por el cesionario, no es necesario consentir de nuevo respecto de la cesión, bastando con el consentimiento prestado inicialmente y que tácitamente se extiende a las cesiones posteriores, esto es, al acceso por terceros a esos datos. En estos supuestos, dice la Agencia, no se infringe el artículo 11; aunque no se haya recabado un nuevo consentimiento para la cesión.

Justamente el que esto sea así deriva de la exigencia de que el fin del tratamiento o la cesión sea explícito y específico. Sólo así, sólo si el afectado pudo conocer con precisión el fin o fines perseguidos con el uso de sus datos, cabe presumir que el tácito consentimiento a la cesión a terceros de sus datos para alcanzar las mismas finalidades.

Cumple ahora abordar los principios de información y consentimiento que cierran el sistema de tutela del derecho fundamental a la protección de los datos personales.

Así, el artículo 5 LOPD describe qué informaciones hay que darle al individuo para obtener y a tratar sus datos. Fundamentalmente, la información se refiere a qué datos son de obligado o suministro o qué consecuencias tiene el que uno se niegue a dar esos datos. Hay que informarle también para qué se quieren los datos y cuál puede ser su posible destino, esto es, las cesiones a terceros. Por tanto, se ha de informar de los usos finales que pueda tener esa información, quién va a tener esos datos, dónde van a estar depositados estos datos y ante quién debo ejercer mis derechos de acceso o posesión, rectificación y cancelación de los datos.

Esencialmente, esta es la información básica que tenemos que ofrecerle a aquella persona cuyos datos estemos utilizando. Esta información puede darse con posterioridad al recabamiento y tratamiento de los datos. Es posible que, por razones que ya se verán, los datos sean obtenidos sin que tenga conocimiento la persona a la que se refieren; cosa muy habitual, por cierto, en la actividad policial. Ahora bien, ello no excusa de que en un momento determinado del procedimiento tengamos la obligación de informarle de esa circunstancia y de que esa información (y su posterior consentimiento, si es el caso) sean condición indispensable para la licitud del empleo de esos datos a efectos probatorios. Dice el apartado 5 del artículo 5 LOPD: «Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido

informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo». Éste será el caso en la mayoría de las ocasiones en las que se tomen imágenes por las FFCCSS. Por su parte la LOV, en su artículo 9, desarrollado en el artículo 21 del Real Decreto 596/1999, de 16 de abril (y Anexo), cubre parte de esa información, aunque resulta necesario complementarla con lo dispuesto en el citado artículo 5 LOPD.

El principio del consentimiento constituye otro elemento capital de la protección de datos. Principio que rige con carácter general, salvo las excepciones expresamente previstas en la LOPD (artículos 6, 11 y 21 LOPD), así como en la LOV. Hay que recabar previamente el consentimiento del interesado para poder obtener y utilizar sus datos. Sin este consentimiento, la obtención y uso de los datos resultan contrarios al derecho fundamental y, por tanto nulo. Piénsese en la utilización como prueba en un proceso penal de datos personales obtenidos mediante la captación de imágenes por un sistema de videovigilancia. Si no se acredita que los datos personales se obtuvieron con consentimiento previo e informado del afectado o no se acredita que se cumple alguna de las excepciones previstas en el artículos 6, 11 ó 21 LOPD, esa prueba debe calificarse de ilícita y prohibida por la lesión del derecho fundamental a la protección de los datos personales, perdiendo así su validez como prueba de cargo.

No se deben de perder de vista otros deberes genéricos previstos en la LOPD, que no siendo parte integrante del contenido del derecho fundamental, su inobservancia puede ser motivo de sanción administrativa y podría suponer la declaración como irregular de la prueba obtenida con infracción de los mencionados deberes. Son tres esos deberes, inscripción de los ficheros de datos en el Registro dependiente de la Agencia española de Protección de Datos, el deber de secreto y confidencialidad del artículo 10 LOPD, y, finalmente, los deberes relativos a las medidas de seguridad del artículo 9 LOPD.

Debe repararse que de acuerdo con el Reglamento de Seguridad aún vigente, Real Decreto 944/1994, de 11 de junio, que todos los ficheros relativos a datos en materia de infracciones penales o administrativas están considerados como de *seguridad alta* (artículo 4 RD 944/1994).[6] Repárese también que los ficheros policiales, si bien tienen un régimen específico, deben ser objeto de inscripción en el Registro General en la Agencia de Protección de Datos, y, además, en el caso de

6. «1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico. 2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el articulo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio. 3. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto. 4. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20. 5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes».

FFCCSS autonómicas o locales, en las agencias autonómicas de protección de datos si existieran. Más adelante veremos las peculiaridades que la propia LOPD en su artículo 22 prevé para el caso de los ficheros con fines policiales. Respecto del deber de secreto del artículo 10 LOPD, éste ya estaría genéricamente previsto para el caso de las actuaciones de las FFCCSS en el artículo 5.5 de la Ley Orgánica 2/1986, de 13 de marzo de FFCCSS. Y que en lo que ahora interesa se ve plasmado en el apartado 2 del artículo 8 LOV.

4. Los derechos de los interesados

El artículo 2 LOPD excluye de su ámbito de aplicación los ficheros sometidos a la normativa sobre protección de materias clasificadas y los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.[7] Además, somete a su legislación específica «los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia»; esto es, la LOV. Sin embargo, esas exclusiones no conllevan una no sujeción a las garantías derivadas del contenido constitucional del derecho fundamental a la protección de datos. En el caso de la videovigilancia se produce una peculiar remisión inversa, por cuanto el apartado 2 de su artículo 2 remite a lo dispuesto en la legislación de protección de datos que en la actualidad es la LOPD. Por lo tanto, a estos efectos, el régimen de protección de datos en materia de videovigilancia es el establecido con carácter general en la LOPD, a pesar de lo que dispone la propia LOPD.

Un aspecto importante es el relativo a los derechos de los interesados frente al tratamiento de los datos personales. La LOPD desarrollar esos derechos, concretando el contenido constitucional del derecho fundamental, que a su vez tienen una ulterior concreción en el Real Decreto 1332/1994, de 20 de junio (complementada con la Instrucción 1/1998 de la Agencia española de Protección de Datos). Esos derechos son, a la información (artículo 5), a consentir (artículo 6), de acceso (artículo 15), de rectificación y cancelación (artículo 16), y de oposición (artículos 6 y 30). De orden legal son los derechos a la impugnación de valoraciones (artículo 13), de consulta del Registro (artículo 14) y a indemnización (artículo 19).

Estos mismo derechos también se contemplan en la normativa especificada de videovigilancia, como recuerdan tanto en la LOV como su Reglamento de desarrollo, Real Decreto 596/1999, de 16 de abril (en adelante, RV) regulan los derechos de información, acceso y cancelación de los interesados («ciudadanos», dice el RV en su Capítulo V) respecto de las imágenes, de los datos obtenidos con oca-

7. El propio precepto señala que: «No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos». Esto no supone su inscripción en el Registro de la Agencia, sino la comunicación de su existencia.

sión de la captación de imágenes y sonido por la instalación de cámaras fijas o por el uso de las cámaras móviles.

Sin embargo, no se contempla ni el derecho de impugnación de las valoraciones, ni el derecho de consulta del Registro General de la Agencia de Protección de Datos. Tampoco contempla los derechos a consentir y de oposición al uso y tratamiento de los datos personales así captados. Sin embargo, en la medida en que el propio artículo 2.2 LOV remite a la LOPD hay que entender que en esa materia también son de aplicación estos preceptos de la LOPD que han sido citados. Por tanto, el régimen de consentimiento u oposición y de consulta al Registro General podría ampliarse también al registro de grabaciones obtenidas a través de la videovigilancia, ejerciéndose en los términos previstos en la LOPD, el Real Decreto 1332/1994, la Instrucción de la Agencia de Protección de Datos 1/1998, y en lo que, sobre el particular, hayan dispuesto las agencias de protección de datos autonómicas en el caso que hayan establecido alguna especificidad en los procedimientos.

Las excepciones a los derechos de las personas constituyen un asunto de primer orden. Debe traerse aquí las reflexiones realizadas por la STC 292/2000. En primer lugar, el artículo 23 LOPD establece un elenco importante de excepciones del derecho de los usuarios en el caso de los ficheros de titularidad pública, por tanto, también en los ficheros utilizados por las FFCCSS (que tienen los suyas propias), que, en general, están todas fundadas en bienes o intereses de rango constitucional.

Dice este artículo 23:

> 1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior (que es el artículo 22) podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.
>
> 2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.
>
> 3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Es necesario aclarar que, fruto de la doctrina del TC sentada en la citada STC 292/2000, la *seguridad pública* a la que se hace mención en el apartado 1 de este artículo 23 y que permitiría excepcional los derechos de los interesados en el caso de ficheros de las FFCCSS, incluidos los formados con las grabaciones tomadas

por los sistemas de videovigilancia, habría que entenderlo ceñido exclusivamente a la prevención y persecución de las infracciones penales.

Así debiera ser, en nuestra opinión, como consecuencia de la declaración de inconstitucionalidad de algunos incisos de los apartados del artículo 24 LOPD. Este precepto establece que:

> 1. Lo dispuesto en los apartados 1 y 2 del artículo 5.º (derechos de información) no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente *el cumplimiento de las funciones de control y verificación de las Administraciones públicas* o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales *o administrativa*.
>
> 2. Lo dispuesto en el artículo 15 (derecho de acceso) y en el apartado 1 del artículo 16 (derechos de rectificación y cancelación) no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de *interés público o ante intereses de terceros más dignos de protección*. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

El TC considero que los incisos en cursiva eran una habilitación en blanco a la Administración Pública para decidir con un grado intolerable de discrecionalidad en qué casos da curso al ejercicio de los derechos de los usuarios y en qué casos no con el fácil expediente de acudir a aquellas excusas genéricas. En este punto el TC ha sido muy contundente. En los FFJJ 17 y 18 de su STC 292/2000 afirmó:

> 17. En el caso presente, el empleo por la LOPD en su art. 24.1 de la expresión «funciones de control y verificación», abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia. De un lado, al habilitar la LOPD a la Administración para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo. Y de un modo tal que, como señala el Defensor del Pueblo, permite reconducir a las mismas prácticamente toda actividad administrativa, ya que toda actividad administrativa que implique entablar una relación jurídica con un administrado, que así será prácticamente en todos los casos en los que la Administración necesite de datos personales de alguien, conllevará de ordinario la potestad de la Administración de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración. Lo que, a la vista del motivo de restricción del derecho a ser informado del art. 5 LOPD, deja en la más absoluta incertidumbre al ciudadano sobre en qué casos concurrirá esa circunstancia (si no en todos) y sume en la ineficacia cualquier mecanismo de tutela jurisdiccional que deba enjuiciar semejante supuesto de restricción de derechos fundamentales sin otro criterio complementario que venga en ayuda de su control de la actuación administrativa en esta materia.

Iguales reproches merece, asimismo, el empleo en el art. 24.2 LOPD de la expresión «interés público» como fundamento de la imposición de límites a los derechos fundamentales del art. 18.1 y 4 CE, pues encierra un grado de incertidumbre aún mayor. Basta reparar en que toda actividad administrativa, en último término, persigue la salvaguardia de intereses generales, cuya consecución constituye la finalidad a la que debe servir con objetividad la Administración con arreglo al art. 103.1 CE.

18. Las mismas tachas merecen también los otros dos casos de restricciones que han sido impugnados por el Defensor del Pueblo, la relativa a la persecución de infracciones administrativas (art. 24.1 LOPD) y la garantía de intereses de terceros más dignos de protección (art. 24.2 LOPD).

El interés público en sancionar infracciones administrativas no resulta, en efecto, suficiente, como se evidencia en que ni siquiera se prevé como límite para el simple acceso a los archivos y registros administrativos contemplados en el art. 105 b) CE. Por lo que la posibilidad de que, con arreglo al art. 24.1 LOPD, la Administración pueda sustraer al interesado información relativa al fichero y sus datos según dispone el art. 5.1 y 2 LOPD, invocando los perjuicios que semejante información pueda acarrear a la persecución de una infracción administrativa, supone una grave restricción de los derechos a la intimidad y a la protección de datos carente de todo fundamento constitucional. Y cabe observar que se trata, además, de una práctica que puede causar grave indefensión en el interesado, que puede verse impedido de articular adecuadamente su defensa frente a un posible expediente sancionador por la comisión de infracciones administrativas al negarle la propia Administración acceso a los datos que sobre su persona pueda poseer y que puedan ser empleados en su contra sin posibilidad de defensa alguna al no poder rebatirlos por resultarle ignotos al afectado. La propia LOPD establece en su art. 13 que los ciudadanos «tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad». Criterios difícilmente compatibles con la denegación del derecho a ser informado del art. 5 LOPD acordada por la Administración Pública con el único fundamento de la persecución de una infracción administrativa.

Por último, el apartado 2 del art. 24 LOPD establece que los derechos de acceso a los datos (art. 15.1 y 2 LOPD) y los de rectificación y cancelación de los mismos (art. 16.1 LOPD) podrán denegarse también si, «ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante... intereses de terceros más dignos de protección». Resulta evidente que tras lo ya dicho, a la vista de que este inciso permite al responsable del fichero público negar a un interesado el acceso, rectificación y cancelación de sus datos personales, y al margen de que esos intereses puedan identificarse con los derechos fundamentales de ese tercero o con cualquier otro interés que pudiere esgrimirse, semejante negativa conlleva abandonar a la decisión administrativa la fijación de un límite al derecho fundamental a la protección de los datos de carácter personal sin ni siquiera establecer cuáles puedan ser esos intereses ni las circunstancias en las que quepa hacerlos valer para restringir de esa forma este derecho fundamental.

(...)

> Como en otra ocasión hemos aseverado, los motivos de limitación adolecen de tal grado de indeterminación que deja excesivo campo de maniobra a la discrecionalidad administrativa, incompatible con las exigencias de la reserva legal en cuanto constituye una cesión en blanco del poder normativo que defrauda la reserva de ley. Además, al no hacer referencia alguna a los presupuestos y condiciones de la restricción, resulta insuficiente para determinar si la decisión administrativa es o no el fruto previsible de la razonable aplicación de lo dispuesto por el legislador (SSTC 101/1991, FJ 3, y 49/1999, FJ 4). De suerte que la misma falta evidente de certeza y previsibilidad del límite que el art. 24.2 LOPD impone al derecho fundamental a la protección de los datos personales (art. 18.4 CE), y la circunstancia de que, además, se trate de un límite cuya fijación y aplicación no viene precisada en la LOPD, sino que se abandona a la entera discreción de la Administración Pública responsable del fichero en cuestión, aboca a la estimación en este punto del recurso interpuesto por el Defensor del Pueblo al resultar vulnerados los arts. 18.4 y 53.1 CE.

Esto tiene cierta importancia porque una cláusula muy similar está prevista en la LOV respecto a las restricciones que el responsable de estos ficheros puede oponer al ejercicio de los derechos de acceso y cancelación de los afectados por un control de videovigilancia. El artículo 9 LOV dispone que podrán denegarse el ejercicio de esos derechos «en función de los peligros que pudieran derivarse para la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se están realizando». Parece que, en una recta aplicación de la doctrina antes transcrita de la STC 292/2000, habría que considerar contrario al derecho fundamental a la protección de datos la denegación del ejercicio de los derechos citados si el motivo de la denegación estriba en la protección de «las necesidades de las investigaciones que se estén realizando», sin más.

5. Las peculiaridades de los ficheros policiales. El artículo 22 LOPD

El artículo 22 LOPD establece:

> 1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.
>
> 2. 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.
>
> 3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los

> datos, a que hacen referencia los apartados 2 y 3 del artículo 7.º, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.
>
> 4. 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.

Éste debe ser, a nuestro juicio, el marco general de los ficheros que contengan imágenes obtenidas a través de sistema de videovigilancia, por cuanto los fines del uso de sistemas de videovigilancia son similares a los que, con arreglo al citado artículo, permitirían la existencia de ficheros de las FFCCSS (artículo 1 LOV). A salvo la imposibilidad de la «rectificación» de ese tipo de datos, se nos escapa qué cualidad pudiere hacer de este tipo de fuente de datos personales un mecanismo para su recabamiento y tratamiento ajeno a lo dispuesto en la LOPD, y más en concreto, de su artículo 22.

5.1. Tipología de ficheros policiales

La LOPD en su artículo 22 parece distinguir entre los ficheros policiales con finalidades administrativas, y aquellos empleados para «fines policiales», dice la norma, y que debieran entenderse referidos a investigaciones de hechos que pudieren ser constitutivos de infracciones penales y/o administrativas.

Los ficheros policiales que tienen finalidad administrativa son tratados como cualquier otro fichero de cualquier otra Administración pública. Estos ficheros están sujetos al régimen general de la LOPD.

Los ficheros con finalidades policiales que regula el artículo 22.2 de LOPD se deben clasificar en aquéllos donde ha habido un previo consentimiento del afectado para que sus datos sean incorporados a ese fichero y sometidos a tratamiento, y aquéllos en los que no hay ese previo consentimiento, y, en consecuencia no hay conocimiento del afectado de su recogida y tratamiento ni previa información. Estos últimos son los que expresamente regula el apartado 2 del artículo 22. Dice ese apartado segundo:

> 2. 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.

Entonces, cabe inducir del artículo 22 LOPD que todo tratamiento de datos efectuado por las FFCCSS que persigan fines administrativos, o que lo hagan de fines policiales que no estén ligados a «la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales» están sujetos al régimen general de la LOPD.

A la vista de lo dicho más arriba, respecto de los derechos de los interesados, el caso de los ficheros con fines policiales que pueden crearse y existir sin previo consentimiento del interesado, y, en consecuencia sin estar informado sobre su existencia y finalidad, plantea serias dudas cuando de procedimientos administrativos (piénsese en el régimen de extranjeros) se trata. Menos dudas plantea, por el contrario, los que se creen en el marco de investigaciones policiales concretas dentro de una instrucción penal.

En nuestra opinión, los ficheros, temporales o permanentes[8] que resulten del uso de videocámaras fijas o móviles se debe encuadrar en el marco del artículo 22 LOPD dada, por lo demás, la coincidencia de fines. El artículo 1 LOV dispone que el objeto de esta Ley es regular «la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad publica». Lo que complementan los artículos 4 y 5 LOV al establecer los motivos que pueden justificar la instalación y/o empleo de cámaras fijas y de equipos de grabación móviles. En le primer caso esos motivos son «asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes»; y en el segundo fijas «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».

El propio artículo 22 contempla el caso de aquellos ficheros policiales que contengan datos de los comúnmente denominados «sensibles» del artículo 7 LOPD: ideología, religión o creencias, afiliación sindical y los que hagan referencia al origen racial, a la salud y a la vida sexual.

---

8. No se olvide que la LOV prevé un régimen específico de conservación de las grabaciones en su artículo 8: «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». Que es desarrollado en detalle por los artículos 18, 19 y 20 RV. No se olvide que conforme a lo dispuesto en el apartado 4 del artículo 22 LOPD: «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». Sin duda para fijar el alcance temporal de esa necesidad será de gran utilidad la rica doctrina del TC sobre el tiempo de la detención del artículo 17.2 CE.

En ese caso, la LOPD acude a la doctrina del peligro cierto, real e inminente para justificar excepcionalmente la obtención de esos datos y su tratamiento por las FFCCSS. Establece el artículo 22 en su apartado 4 que la recogida y tratamiento de datos sensibles por las FFCCSS sólo podrá realizarse «en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta». Así pues, podrá crearse un fichero policial, o podrá contener este tipo de datos, si cabe acreditar la existencia de un riesgo cierto, inminente y real que requiera su empleo, cuya evidente formalización es la existencia de una investigación concreta. No basta, pues, la mera sospecha, sino la existencia de indicios racionales de que existe ese peligro, y así habrá de razonarse en el marco de una investigación, so pena de infringir el principio de proporcionalidad (artículo 6 LOV y artículo 4 LOPD). También este criterio debe aplicarse al uso de videocámaras (repárese en las grabaciones de una manifestación pública en la que quepa luego asociar a determinadas personas con determinadas ideologías o filiaciones sindicales o políticas, como sucedía en el caso de la STC 37/1998 que más abajo es objeto de unas observaciones).[9]

5.2. Creación de los ficheros y responsable del tratamiento

Los ficheros policiales no están exceptuados del régimen general de creación, modificación y supresión de ficheros por las Administraciones públicas (artículo 20 LOPD). Por lo tanto, la creación de ficheros por la policía con ocasión de sus actividades tanto en la prevención como en la persecución de infracciones administrativas o penales, también los derivados de la videovigilancia, están sujetos a la previa existencia de una disposición de carácter general que regule la existencia, contenido, uso, destino, modificación y forma de supresión del fichero, en este caso del fichero policial. Y esa disposición no es, claro está, la LOV o el RV. Si no hay esa norma de creación, ese fichero es contrario al derecho fundamental a la protección de datos.

La LOPD ha creado la figura del responsable del fichero o del tratamiento que define su artículo 3 d) en los siguientes términos: «persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento». Hay acuerdo sobre el hecho de que esta figura no se ha de identifica con el *propietario* del fichero, sino con quien tenga atribuido el poder jurídico de disposición sobre él. En este sentido, la LOV identifica a quien debiera tenerse por responsable del fichero o tratamiento derivado del uso de videocámaras en su artículo 8.4 al señalar: «reglamentariamente la Administración competente determinará el órgano o autoridad gubernativa que tendrá a su cargo la custodia de las imágenes obtenidas y la responsabilidad sobre su ulterior desti-

9. No conviene olvidar que el artículo 55 CE relativo a la suspensión general o singular de derechos fundamentales no contempla el derecho a la intimidad o a la protección de datos. Con carácter general en esta materia es de cita obligada las SSTC 199/1987 y 71/1994. Y no se olvide que el propio artículo 2 LOPD excluye de su ámbito lo relativo a la lucha antiterrorista y contra la delincuencia organizada.

no, incluida su inutilización o destrucción. Dicho órgano será el competente para resolver sobre las peticiones de acceso o cancelación promovidas por los interesados».

Así definida esta «autoridad» responde con meridiana claridad al responsable del fichero o del tratamiento previsto en la LOPD y sobre el que pesan una serie de obligaciones ya descritas en este trabajo páginas más arriba. Cabría sugerir el empleo de la norma reglamentaria que la identifique para, precisamente, establecer los términos de creación y uso del fichero derivado del empleo de videocámaras, cumpliendo con la previsiones del artículo 20 LOPD, entre las que se cuenta justamente la identificación del responsable (artículo 20.1 f) LOPD).

5.3. Comunicación de datos contenidos en ficheros policiales

El artículo 21 de la LOPD afecta también a esta materia, pues regula con carácter general los términos en los que se pueden ceder datos entre Administraciones públicas. Las reglas de la cesión, esto es, de la comunicación de datos entre Administraciones, por tanto entre los distintos FFCCSS y de éstos con otros entes públicos, son: en primer lugar, que deben estar previstas en la disposición general que regule la existencia de los ficheros policiales; en segundo lugar, sólo caben cesiones no previstas en la disposición de creación del fichero si los datos son comunicados a otra Administración pública para ejercer competencias similares o sobre la misma materia que las ejercidas por la Administración cedente, o lo prevé una norma con rango de ley orgánica (STC 290/2000); en tercer lugar, las cesiones deben ser conocidas y consentidas por el afectado; no obstante el consentimiento previo de la persona cuyos datos se van a ceder sólo es necesario en el caso de que se cedan para ejercer competencias distintas o sobre materias diferentes, si esa cesión no esté prevista en la disposición general de creación del fichero o en una norma con rango de ley orgánica.[10]

En consecuencia, y advertidos de que los lugares de tránsito público no son «fuentes accesibles al público»[11] que autoricen una comunicación de imágenes de personas sin su consentimiento (artículo 11 b) LOPD), las FFCCSS sólo podrán ceder sin el previo consentimiento de los afectados las grabaciones y ficheros de

---

10. Criterio que a nuestro juicio encajaría en lo dispuesto en el artículo 11 LOPD apartado a) (cesiones autorizadas por ley) y d) («Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas»).

11. Artículo 3 j) LOPD: «Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación».

grabaciones de imágenes o sonidos obtenidos con sistemas de videovigilancia a otras Administraciones públicas si así está previsto en la disposición general de creación del fichero, que habrá de tener en este caso rango de ley orgánica al tratarse de una restricción de un derecho fundamental (STC 290/2000); o si «la Administración cesionaria es el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas» (artículo 11 d) LOPD).[12]

Si bien el apartado 3 del artículo 8 LOV prohíbe las cesiones o copias de las imágenes y sonidos videograbadas, establece las excepciones tan severa regla remitiendo a su apartado 1 según el cual las grabaciones podrían ser, en lo que ahora nos interesa, cedidas si están «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». Lo que se corresponde con lo dispuesto en el artículo 7 LOV.

En este sentido el artículo 7 LOV regula la cesión de los datos derivados del empleo de las videocámaras de manera ajustada a las previsiones de la LOPD. Ese precepto establece que si las imágenes hubieren captado hecho que pudieran tener relevancia penal, serán comunicados a la autoridad judicial o al Ministerio Fiscal. Cesión que no requiere del consentimiento previo de los afectados como así resulta del artículo 11. 2 d) LOPD. Ese mismo artículo 7 en su apartado 2 hace lo propio en el caso de que los hechos pudieren ser constitutivos de una infracción administrativa relacionada con la seguridad ciudadana. En este caso, y con toda cautela, cabría dar cobertura a esta cesión, e incluso que pudiere tener lugar sin el previo consentimiento del afectado, aplicando lo dispuesto en el artículo 21.1 y 4 LOPD; esto es, se ceden datos para alcanzar los mismos fines referidos a la seguridad ciudadana que motivaron su recogida (identidad de materias y fines). Recuérdese que la Agencia estatal de Protección de Datos considera que si hay identidad de fines entre los sucesivos usos a los que se destine el dato, sólo hace falta contar con el consentimiento para la primera utilización.

Merece que nos detengamos un instante en la comunicación de datos entre unidades del mismo Cuerpo y entre distintos CCFFSS. En el primer caso, a falta de criterio jurisprudencial o de las Agencias de protección de datos, bien parece que haya de considerarse cesión cuando el acceso a los datos se autoriza a cuerpos o unidades de policía que no cabe considerar integrados orgánica y/o funcionalmente en aquel que obtuvo los datos. A nuestro juicio, la personalidad jurídica autónoma de la unidad o cuerpo es el criterio que debe permitirnos distinguir entre aquellos que pueden considerarse una misma Administración pública y aquellos que pertenecen a Administraciones distintas, de forma que sólo habría cesión de datos en este segundo caso.

---

12. Al margen claro está de la comunicación de datos disociados o con fines históricos, científicos o estadísticos, artículo 11 e) y apartado 6.

La cooperación internacional en la lucha contra el terrorismo y las formas organizadas de delincuencia constituyen implican diversas formas de cesión de datos entre FFCCSS de distintos Estados. Aunque quizá no sea éste el lugar conveniente para abordar este asunto, indudablemente posee un relieve de primer orden. De un lado, por la intensidad y extensión del intercambio de datos que conlleva el Sistema de Información Schengen,[13] que no se limita al intercambio de datos en materia de terrorismo y bandas organizadas de delincuencias; y de otro, la necesidades derivadas de la cooperación judicial y policial internacional. Siendo la última expresión de este fenómeno la reciente y no menos polémica Directiva 2006/24/CE del Parlamento Europeo y el Consejo, de 15 de marzo de 2006, sobre la conservación de datos generales o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.[14]

La LOPD regula en sus artículos 33 y 34, Título V, el movimiento internacional de datos. Esta regulación se reduce a una norma muy simple: no se pueden transferir datos obtenidos en España a otro Estado, sea un Estado de la Unión Europea o no, sin que haya una declaración de lo que se conoce como «puerto seguro». Y por tales debe entenderse aquellos «países que... proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas» (artículo 33.1 LOPD).

Esa declaración se sujeta a un procedimiento reglado en el propio artículo 33 LOPD[15] y que es competencia de la Agencia estatal de Protección de Datos. El artículo 34 LOPD establece las siguientes excepciones, relevantes para las cuestiones tratadas en este trabajo, a lo dispuesto en el citado artículo 33:

> a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
>
> b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

---

13. Conciente el legislador internacional de ello el Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 relativo a la supresión gradual de los controles en las fronteras comunes (al que se adhirió España por Acuerdo de 25 de junio de 1991), dedica su Capítulo III (artículos 102 a 118) a la protección de datos.

14. Cuyo artículo 7 se refiere a la «protección y seguridad de los datos» con una genérica y un tanto confusa remisión a la Directiva 95/46/CE y a la 2002/58/CE.

15. «El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países».

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

En ellas, en especial, la letra k) y, en su caso, las letras a) y b), encontraría plena acogida lo regulado en el Convenio Schengen y los distintos acuerdos de cooperación judicial y policial como los EUROPOL y EURODAC, relativo este último al intercambio de huellas dactilares respecto de los peticionarios de asilo con el fin de establecer cuál es el tercer país responsable en la aceptación y tramitación de las peticiones de asilados.

5.4. Impugnación de valoraciones y prueba

Detengámonos un instante en el derecho a las impugnaciones de valoraciones regulado en el artículo 13 LOPD. En el trabajo policial los datos que obtenemos ante sospechosos suelen utilizarse para un definir un perfil o para valorar el comportamiento de un sospechoso. A partir de ahí, podemos establecer si estamos ante hechos que pueden ser objeto de investigación y, por tanto, de la apertura del oportuno procedimiento sancionador en el caso de infracciones administrativas o del testimonio al Ministerio Fiscal o la comunicación al Juez de Instrucción para iniciar la oportuna instrucción penal en el caso de que los hechos puedan ser constitutivos de una infracción penal. Esta situación plantea alguna dificultad. Si este tipo de valoraciones en las que se establecen perfiles de personas a partir de los datos que de ella se han obtenido, y acaso sea en esto en lo que consisten las deducciones obtenidas de una grabación videográfica, no solo pueden ser impugnados por la persona sujeta a esa *valoración*, y por tanto perseguir la nulidad de las actuaciones administrativas seguidas con ocasión de esa valoración, sino que, además, como dispone el apartado último del citado artículo 13 LOPD, posee un valor probatorio disminuido. Dice ese apartado que «la valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado». Quizá convenga darle a este precepto una interpretación restrictiva y ceñida al ámbito administrativo, de modo que serían las actuaciones de la policía administrativa de seguridad y el ámbito del régimen sancionador administrativo donde esa «valoraciones» poseerían esa calidad disminuida; no así las derivadas de la actuación de la policía judicial.

Justamente, en el marco de las actuaciones como *policía judicial*, la grabación de imágenes y sonidos puede tener valor probatorio, pero en ciertas condiciones sólo. No cabe duda de que la captación de imágenes y sonidos a través de videocámaras o cualquier otro sistema, o la obtención de datos personales a través de la intervención de cualquier tipo de comunicación personal (sea *analógica*... —teléfono de hilo, postal—, sea *digital* —internet, sms—), además de su valor como dili-

gencia de investigación, también podrá tenerlo como prueba preconstituida, exactamente igual que las escuchas telefónicas o las diligencias dentro del registro de un domicilio.

Si así es, su régimen debe ser idéntico al de las pruebas preconstituidas y sumariales respecto de las que hay una rica y sólida jurisprudencia constitucional relativa a su valor y las garantías de las que debe estar rodeada su práctica. El medio de captación o de comunicación no altera en nada el régimen constitucional de garantías de las pruebas preconstituidas.

5.5. La STC 37/1998 (caso del piquete del sindicato LAB) y otras de interés

Pocas ocasiones ha tenido el TC para pronunciarse sobre esta materia. Quizá la merecedora de cita es la STC 37/1998, caso del piquete del sindicato LAB. En esta resolución, el TC se pronunció sobre el caso de una patrulla de la Ertzaintza que, en el control que hacían de la actuación de un piquete informativo del sindicato LAB, tomó fotografías y grabó en video a las personas que formaban parte del piquete.

El TC dictó una sentencia aplicando a la actuación de la Administración pública lo que previamente había dicho con carácter general para el supuesto de la instalación de videocámaras y de sistemas de control y de vigilancia en el ámbito de las relaciones laborales en las SSTC 98/2000, caso Casino de La Toja, y 186/2000, caso Economato de ENSIDESA. En el primero de estos casos se habían instalado cámaras para captar las conversaciones de los empleados y de los clientes del casino, y en el segundo se habían instalado unos micrófonos en el economato de aquella industria. El TC en ambos insistió en la proporcionalidad de las medidas. Reconoció que había un fin constitucional para establecer estos sistemas de vigilancia y control, pero siempre que sean proporcionados al riesgo que se desea prevenir. En el caso piquete LAB, donde no se acreditó un riesgo cierto ni para la seguridad y ni para el orden público, el TC entendió que la medida de grabación y de control era desproporcionada y por lo tanto lesiva del derecho a la propia imagen de los participantes en el piquete informativo.

Las SSTC 70/2002 y 123/2002 abordan en España el denominado *comptage* en los supuestos de intervención de las comunicaciones telefónicas (y algo se podrá importar para el caso de la conservación de los datos por los operadores de telefonía móvil y para los proveedores de acceso a internet). En estos casos se planteaba la legitimidad constitucional de que la policía pudiera acceder sin necesidad de una autorización judicial previa, expidiendo un simple oficio a la compañía de telefonía correspondiente, a los datos relativos a los números de teléfono que habían llamado al intervenido y/o a los que éste había llamado. Los recurrentes consideraban que ese acceso a esos datos sin autorización judicial o consentimiento de los titulares de los números de teléfono vulneraba el derecho al secreto de las comunicaciones del artículo 18.3 CE.

El argumento que utilizó en ambos casos el Abogado del Estado para defender la actuación policial y la corrección de esas diligencias de investigación, que se emplearon con posterioridad como pruebas de cargo en las vistas orales de

ambos procesos penales, es que no afectaban al secreto de las comunicaciones porque el secreto de las comunicaciones solo garantizaba el contenido de la comunicación y no los datos objetivos.[16] Es decir, a su juicio, el derecho al secreto de las comunicaciones no se extendería la identidad de los intervinientes en la comunicación. Por tanto, según el Abogado del Estado, el mero conocimiento de los números de teléfono a los que se llama o de los que se reciben llamadas no afectaba para nada al secreto de las comunicaciones. Pero, añadimos ahora nosotros, sí afecta al derecho fundamental a la protección de los datos personales. Aspecto en el que el TC, por cierto, no repara.

Debe hacerse notar que el TEDH ya desde el caso Malon, de 2 de agosto de 1984, ha dicho que forma parte de la comunicación y de su secreto, no solo el contenido de lo que se dice sino también la identidad de los destinatarios y partícipes en esa comunicación. Esta doctrina ha sido acogida de modo rotundo por el Tribunal Constitucional en las SSTC 70/2002 y 123/2002. El TC mantiene la misma posición que el TEDH y considera, por lo tanto, que también se lesiona el derecho fundamental al secreto de las comunicaciones si se accede a ese tipo de datos identificadores de los partícipes en las comunicaciones. Esta identidad no tiene que ser necesariamente la identidad personal de los comunicantes, basta con que se obtenga el número o el lugar desde donde se hace la llamada o la antena que ha dado la cobertura para la comunicación. Así pues, sujetos esos datos a la garantía del secreto de las comunicaciones, o hay consentimiento de los afectados para obtenerlos y usarlos, o hay un supuesto de flagrancia (circunstancia de muy difícil concurrencia en el caso de estos datos y a las intervenciones de comunicaciones privadas), o hay autorización judicial previa.

En lo único que el TC ha sido condescendiente con la actuación policial es que para el caso de este tipo de datos no es necesario que la autorización judicial tenga forma de auto, bastando la providencia, siempre que contenga una sucinta motivación en la que se expongan la razones por las cuales se autoriza a la policía a acceder a ese tipo de información.

No deseamos concluir este apartado sin llamar la atención sobre el hecho de que, aun en el caso de que no se hubiese incorporado a nuestra doctrina constitucional el *comptage*, el derecho fundamental a la protección de los datos personales hubiese ofrecido tutela sobrada para este tipo de accesos.

Por último, pero no menos importante recordemos que el TC ha matizado esa idea muy extendida de que la captación de imágenes en lugares públicos no afecta al derecho fundamental a la propia imagen. El TC ha venido a decir en la STC 139/2001 que, si el derecho a la propia imagen supone un control sobre el uso y destino de la imagen física, el que se capte en un lugar privado o en un lugar públi-

16. Esta ha sido también la línea argumental esgrimida por la Unión Europea y el Ministerio del Interior español para sostener la constitucionalidad de las medidas de retención de datos que finalmente se han fijado en la ya citada Directiva 2006/24/CE de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la presentación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Véase con carácter general las Conclusiones de la Presidencia del Consejo Europeo de Bruselas de 16 y 17 de junio de 2005 (puntos 17 y siguientes).

co tendrá relevancia a los efectos de graduar la proporcionalidad de la medida de restricción, pero no para determinar si se afecta o no el derecho a la propia imagen de la persona.

6. Y ALGUNAS CONSIDERACIONES FINALES

Dejando a un lado los problemas que la LOV y su RV puedan plantear desde distintas perspectivas, y que han sido sobradamente subrayados por los especialistas en la materia, el uso de estas técnicas para el desarrollo de la actividad policial, sea en sus funciones de *policía administrativa* o en las de *policía judicial*, entrañan serios riesgos para la protección de datos personales. Repárese en que ya hay tratamiento de datos personales, habida cuenta de que las imágenes y los sonidos lo son, y creación de ficheros, desde el instante en que la LOV permite conservar las grabaciones durante un mes. En ese caso, resulta ineludible tener en cuenta las reglas del artículo 22 LOPD.

Lo curioso del asunto, y que no puede pasar inadvertido, es que dada la regulación de la LOV, la instalación de sistemas de videovigilancia, fijos o móviles, no parece estar prevista para el ejercicio de las funciones propias de la *policía judicial*, sino más bien como instrumento complementario en el ejercicio por las FFCCSS de las propias de *policía administrativa*. Justo aquí se ahn centrado todos los reparos que hasta el momento se han puesto, desde la perspectiva constitucional, al uso de esta técnica.

Así las cosas, parece inevitable concluir que en el caso de que se deseen utilizar estas técnicas (emplear videocámaras para grabar a sospechosos en el marco de una instrucción penal) o servirse de los datos obtenidos por su uso (emplear las grabaciones obtenidas por las cámaras instaladas en un edificio público) resultará indispensable obtener una autorización judicial previa, si no el consentimiento de los afectados.

Que así sea, deriva del hecho de que, en primer lugar, el uso de estos sistemas de videovigilancia (por mucho que el apartado 1 del artículo 2 LOV lo pretenda negar respecto de otros derechos fundamentales) supone una restricción del derecho a la protección de datos en el caso de que se conserven las grabaciones por el tiempo que sea; en segundo lugar, pueden constituir restricciones del secreto de las comunicaciones, porque la grabación puede estar interfiriendo una comunicación privada; y, en tercer lugar, porque, además (e insistimos que a pesar de lo dispuesto ene l artículo 2.1 LOV, pues no es el Legislador, ni siquiera el orgánico, quien dispone sobre si una actuación de un poder público es o no limitativa y en su caso lesiva de un derecho fundamental), es una restricción del derecho de la propia imagen, por cuanto se captan imágenes de personas sin contar con su consentimiento.

Quisiera finalizar mi intervención realizando algunas reflexiones sobre la videovigilancia privada. Cabe señalar que la utilización de sistemas de captación en el caso de la seguridad privada no tiene regulación. Ni la Ley ni el Reglamento de Seguridad Privada (Ley 23/1992, de 30 de julio, y Real Decreto 2364/1994, de 9 de diciembre) han regulado esta materia, salvo en lo relativo a las entidades banca-

rias, donde se autoriza su instalación. No es el momento ni hay tiempo para hacer una reflexión sobre esta materia. Quede aquí apuntada, y sirva de reto para que se someta al estudio que requiere, sin perder de vista que las imágenes captadas por estos sistemas han demostrado una probada utilidad en la persecución de hechos delictivos.[17]

7. Bibliografía

Con carácter general consúltense los libros:

Guichot, E., *Datos personales y Administración pública*, Thomson-Civitas/APDCM, Madrid, 2005.

Martínez Martínez,R., *Una aproximación crítica a la autodeterminación informativa*, Thomson/Civitas-APDCM, Madrid, 2004.

Messía de la Cerda Ballesteros, J.A., *La cesión o comunicación de datos de carácter personal*, Thomson-Civitas/APDCM, Madrid, 2003.

Con carácter específico consúltese:

Barcelona Llop, J., «El Secreto policial. Acceso a archivos y registros de la policía. Los ficheros automatizados de las Fuerzas y Cuerpos de Seguridad. A propósito de la Ley Orgánica 4/1997, de 4 de agosto, llamada de videovigilancia», *Actualidad Administrativa*, núm. 13, 1998, marginal 205.

González Urdinguio / González Gutierrez de León, «La videovigilancia en el sistema democrático español. Análisis crítico de la Ley Orgánica 4/1997, de 4 de agosto», *Revista de la Facultad de Derecho de la Universidad Complutense,* núm. 89, 1998, p. 105 y ss.

Martínez Martínez, R., «Videovigilancia, seguridad ciudadana y derechos humanos», *Claves de la Razón Práctica*, núm. 89, 1999, p. 40 y ss.

— «Videovigilancia en lugares públicos», *Repertorio Aranzadi del Tribunal Constitucional,* núm. 17, 2000, p. 31 y ss;

Magrot Servet, V., «Consideraciones sobre la nueva Ley que regula la utilización de las videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado», *Revista del Poder Judicial,* núm. 47, 1997, p.. 277 y ss.

Padrós Reig, C., «Videovigilancia y Estado autonómico. Comentario a propósito de la actividad normativa de despliegue de la ley Orgánica 4/1997», *Revista de Administración Pública*, núm. 151, 2000, p. 465 y ss.

Ull Salcedo, M.V., «El derecho a la intimidad como límite a la videovigilancia» en *Revista de Derecho Político*, núm. 63, 2005, pp. 177 y ss.

17. Véase el caso de la STC 206/2003 sobre el uso como prueba de las cintas con imágenes captadas por un cámara instalada en el lugar en el que estaba un cajero automático de una entidad bancaria.