VIDEOVIGILANCIA PRIVADA EN LUGARES DE ACCESO PÚBLICO Y DERECHO A LA PROTECCIÓN DE DATOS: EL CASO ALEMÁN

Ana Gude Fernández

1. SEGURIDAD VERSUS LIBERTAD: LA VIDEOVIGILANCIA

La libertad y la seguridad son bienes constitucionales de primer orden en la medida que constituyen un presupuesto indispensable para el efectivo disfrute y cumplimiento de todos los demás. Los textos constitucionales y las declaraciones de derechos afirman que toda persona tiene derecho a la libertad y seguridad, sin embargo, se trata de un principio de no fácil realización. En la práctica se presentan como un binomio en constante tensión[1], en donde siempre es necesario sacrificar en mayor o menor medida una de sus partes.

Los dos derechos constitucionales en juego deben ser ponderados con el fin de buscar un equilibrio entre ellos para lograr que los medios utilizados para su tutela no causen un deterioro al propio Estado. Estas valoraciones se

[1] FRANKLIN, B. «Quien limita la libertad para ganar seguridad, perderá al final ambas».

han de realizar, en primer término, por el legislador, que debe pronunciarse necesariamente a propósito de las técnicas que puedan suponer una restricción de derechos. A continuación, los jueces y el órgano administrativo autorizante, intervendrán con un importante papel, enjuiciando la adecuación de las medidas potencialmente limitativas.

En la actualidad, el uso de las modernas tecnologías y, en particular, la aplicación de los sistemas de videovigilancia para garantizar la seguridad han contribuido a la prevención y persecución del delito, pero al mismo tiempo, no cabe duda de que han sido una fuente generadora de problemas: sus indudables ventajas han supuesto en muchos casos un sacrificio excesivo de no pocos derechos y libertades[2].

La captación y/o el tratamiento de imágenes con fines de observación es una práctica muy extendida en nuestra sociedad y se ha convertido en una alternativa clara a la vigilancia humana durante las 24 horas, que hoy resulta imposible de mantener por el elevado coste económico que supondría. El desarrollo de la electrónica y con ella de los sistemas de control ha permitido la instalación de cámaras en múltiples ámbitos o eventos, como son, por ejemplo, los lugares dedicados al transporte público; las concentraciones multitudinarias, los encuentros deportivos o las grandes manifestaciones; los locales dedicados a exposiciones de mercancías o de objetos de gran valor económico; las grandes superficies comerciales, etc.

La prevención de incidentes junto con la seguridad han sido dos de los principales objetivos que se pretenden alcanzar con el emplazamiento de estos equipos técnicos, cuyas imágenes pueden ser observadas en directo pero cada vez más son analizadas por un *software* especializado. Los empresarios acuden también a estos nuevos métodos para verificar el cumplimiento por los trabajadores de sus obligaciones y deberes laborales. Finalidades todas ellas dignas de protección jurídica pero que obviamente han de satisfacerse cumpliendo requisitos legales estrictos.

El pueblo otorga a sus representantes un mandato para que garanticen la seguridad y deposita su confianza para que las medidas adoptadas no se apliquen en detrimento de los derechos y libertades tutelados por la ley. Las autoridades han de asumir la responsabilidad de controlar la utilización transparente de los instrumentos empleados para garantizar la seguridad. ¿Derecho a la seguridad, derecho a la protección de la vida privada?. ¿Hay alguna prioridad?. ¿Uno se impone al otro?. En teoría, los ciudadanos deberían poder gozar de ambos bienes jurídicos en una sociedad democrática, de la forma en que se tutela tanto por los ordenamientos nacionales e internacionales sin tener que optar por uno de ellos[3].

[2] Sobre este tema, vid. el artículo de Roggan, F., «Die Videoüberwachung von öffentlichen Plätzen», en *Neue Zeitschrift für Verwaltungsrecht*, nº 20, 2001, pp. 134 y ss.

[3] Marcus, M., «El desafío: conciliar el uso de la videovigilancia y las libertades individuales», *Ciudadanos, ciudades y videovigilancia. Hacia una utilización democrática*

El derecho a la intimidad no tiene que desaparecer en cuanto salimos de nuestros domicilios. Nadie discute que sea posible la existencia de un mismo nivel de privacidad en la calle que en la habitación de una casa, sin embargo parece lógico que también podamos disfrutar de ella cuando realizamos nuestras actividades en la vía pública. Por sus propias características, la videovigilancia de estos espacios atenta contra este derecho de la personalidad, porque somos observados de forma constante cada vez que paseamos por la calle o accedemos a uno de esos locales vigilados.

Las cámaras nos impiden conservar nuestro anonimato y nos convierten en visibles para el ojo atento de otros particulares o incluso del propio Estado. Ser examinados por una cámara, que en muchas ocasiones conserva una copia de la grabación, no es lo mismo que ser contemplados por una persona. En el primer caso, la vigilancia es con carácter general más prolongada, más intensa, más detallada. No permite interrogar a la persona que se encuentra detrás, y en consecuencia, es difícil para nosotros saber cómo responder a ese seguimiento o decidir qué podemos hacer al respecto. Desconocemos qué imágenes obtenidas por las cámaras se conservarán o quién tiene acceso a ellas, tampoco, en consecuencia, podemos tener la certeza de que no sean malinterpretadas o utilizadas de modo inaceptable[4].

El filósofo y criminólogo Andrew von Hirsch ha descrito de manera muy gráfica lo que representa ser examinado a través de un sistema de videovigilancia: «es como desarrollar nuestras actividades en un lugar con un espejo, uno sabe que nos están observando detrás de él, pero no necesariamente disponemos de la información de quiénes son o qué están buscando los que están del otro lado»[5]. Además de constituir una obvia intrusión en la esfera privada, debido a la incertidumbre que su utilización genera plantean una grave amenaza a nuestra intimidad en el espacio público. Por eso, algunas personas sienten inseguridad y modifican su forma de actuar[6], no porque crean que estén haciendo algo malo sino porque no desean llamar la atención o correr el riesgo de que sus acciones sean malinterpretadas. En este sentido Giovanni Buttarelli, Supervisor adjunto europeo de Protección de datos, ha advertido que: «Ser observado cambia el modo de comportarse.

---

y responsable de la videovigilancia, p. 15. En http://cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Publication/CCTV_Publication_ES.pdf

[4] Good, B. J., «Videovigilancia y derechos humanos», *Ciudadanos, ciudades y videovigilancia. Hacia una utilización democrática y responsable de la videovigilancia*, p. 30. En http://cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Publication/CCTV_Publication_ES.pdf

[5] Good, B. J., «Videovigilancia y derechos humanos» *op. cit.* (nota 4), pp. 30-31.

[6] Según Zöller la inseguridad acerca del porqué y del cuando alguien va a ser observado conduce a una parte de la población a sufrir una especie de miedo a la videovigilancia (*Überwachungsdruck*). En Zöller, M. A., «Möglichkeiten und Grenzen polizeilicher Videoüberwachung», *Neue Zeitschrift für Verwaltungsrecht*, nº 24, 2005, p. 1238.

Por cierto, cuando somos contemplados muchos de nosotros censuramos lo que decimos o lo que hacemos y ciertamente tal es el efecto de una vigilancia continua y generalizada. Saber que cada movimiento y que cada gesto está controlado por una cámara puede tener un impacto psicológico y cambiar nuestro comportamiento, lo cual constituye una intrusión en nuestra privacidad»[7].

Por ello, y a la vista de todas estas consideraciones, los expertos en la materia han llegado a la conclusión de que tanto los operadores como los administradores de los sistemas de vídeo deben garantizar que la vigilancia del espacio público no anule el derecho a la intimidad, ni modifique completamente el modo en que la gente disfruta del mismo, lo que se traduce en el cumplimiento de los siguientes requisisitos. En primer lugar, es esencial que cada sistema sea utilizado conforme a las restricciones que impone el ordenamiento jurídico, realizando todos los esfuerzos necesarios para evitar abusos en la utilización de las cámaras. En segundo lugar, es preciso que estos instrumentos sólo se empleen para los objetivos inicialmente previstos, evitando de este modo el fenómeno de *function creep* (desvío gradual de la función inicial). Finalmente, es necesario actuar con los sistemas de modo abierto y transparente, de manera que sus operadores o usuarios respondan directamente al público[8]. No cabe duda de que la instalación de las cámaras de vigilancia en el espacio público puede generar consecuencias negativas en la vida privada de las personas. Sin embargo, si existiese una legislación adecuada, garantizadora de los derechos de los afectados, se podría disminuir la pérdida de intimidad, al mismo tiempo que se alcanzaría una vigilancia lícita y eficaz de los lugares de acceso público[9].

En realidad, la conciliación entre seguridad y libertad está lejos de ser algo obvio. La libertad es un derecho «débil» que se relativiza fácilmente de cara a la problemática de la inseguridad. La videovigilancia es una tecnología que suscita muchos interrogantes: ¿Qué se puede filmar?. ¿Hay un derecho a la vida privada en el espacio publico?; y en caso afirmativo ¿cómo proteger este derecho?. ¿Es posible evitar la discriminacion de algunos grupos y de qué forma se puede poner esta herramienta de vigilancia a disposición de toda la población?. ¿Qué hacer para que la videovigilancia funcione y cuando recurrir a otros instrumentos?. ¿De qué manera se puede utilizar la videovigilancia con los ciudadanos como herramienta para prevenir la criminalidad y garantizar la tranquilidad pública?[10].

---

[7] Good, B. J., «Videovigilancia y derechos humanos», *op. cit*. (nota 4), p. 30.

[8] Good, B. J., «Videovigilancia y derechos humanos», *op. cit*. (nota 4), p. 31.

[9] Good, B. J., «Videovigilancia y derechos humanos», *op. cit.* (nota 4), pp. 27-30.

[10] Marcus, M., «El desafío: conciliar el uso de la videovigilancia y las libertades individuales», *op. cit*. (nota 3), p. 16.

2. ALGUNOS APUNTES ACERCA DE LA VIDEOVIGILANCIA EN INGLATERRA Y ALEMANIA

Las videocámaras se encuentran dispersas en pueblos y ciudades de todo el mundo para la contemplación del espacio público y privado. En los últimos veinte años se han vuelto cada vez más frecuentes. Aunque su expansión representa una tendencia internacional a partir de los años noventa, es cierto también que existen notables diferencias entre los países, incluso dentro del viejo continente. Francia, Alemania, Austria[11], Holanda e Italia tardaron tiempo en adoptar estas técnicas de imagen cuya utilización lideró de manera indiscutible el Reino Unido.

Las primeras cámaras se introdujeron en Inglaterra en los años 60 para el control del tráfico, garantizar la seguridad de los centros comerciales, supervisar las manifestaciones políticas y sobre todo, luchar contra la delincuencia. El número de delitos se había incrementado de forma progresiva a partir de los años sesenta. Las estrictas medidas policiales adoptadas durante el gobierno de Margareth Thatcher (1979-1990) no eran suficientes para reducir la delincuencia. En 1972 se contabilizaron alrededor de 1,7 millones de delitos; en 1981, 3 millones; en 1996, 5 millones y en el año 2002 alrededor de 5,8. También Escocia vivió un fenómeno muy parecido de aumento de infracciones penales. En este contexto de grave inseguridad ciudadana se generó una especie de consenso nacional: los distintos partidos y también los medios de comunicación social reivindicaron la necesidad de introducir nuevas armas de lucha contra la delincuencia.

Los sistemas de videovigilancia[12] se convirtieron en la alternativa adecuada y de manera sorprendentemente rápida se extendieron por todo el país. Dos factores explican principalmente este fénomeno. Por un lado, la ausencia de una regulación jurídica en el campo de la videovigilancia. La Ley de Protección de datos del Reino Unido, de 1984, se aplicó únicamente al procesamiento digital y dejó de lado los sistemas analógicos que eran los que con mayor frecuencia se instalaban los primeros años. Es más, la sobre el Orden público y la Justicia criminal, de 1994, autorizó explícitamente la incorporación de «equipos para registrar imágenes visuales de eventos en cualquier lugar del país», aquí porque, además, estaban exentos de pagar las licencias costosas del sistema por cable. El marco regulatorio no fue modificado hasta muy tarde. La implementación de la Directiva sobre la Protección de datos de la Unión europea, no se produjo hasta 1998, a través de la modernización del

[11] KNIEPERT, T., sostiene que Alemania y Austria son los países europeos más críticos con la videovigilancia. *Videoüberwachung im öffentlichen Raum*, Regensburg, 2010, p. 17. En http://www.sebastianbartsch.de/data/Bachelorarbeiten/Video%C3%BCberwachung%20im%20%C3%B6ffentlichen%20Raum.pdf

[12] HEMPEL, L., «Zwischen globalen Trend und Nationaler Varianz», *Polizeitlicher Videoüberwachung öffentlicher Raüme*, Duncker&Humblot, Berlin, 2007, pp. 17 y ss.

Acta, y hasta el año 2000 no se incluyó el Convenio europeo de Derechos humanos en el Acta de Derechos humanos nacional.

Por otro lado, dos sucesos acontecidos en el país con una enorme repercusión mediática contribuyeron de manera notable al desarrollo de estas técnicas: el secuestro de James Bulger, en julio de 1993, y unos atentados que años más tarde, pero en ese mismo mes, se llevaron a cabo en algunos medios de transporte público en la ciudad de Londres.

El primer hecho tuvo lugar en 1993. James Bulger era un niño de 2 años que fue torturado y posteriormente asesinado en la vía del tren por otros dos menores de 9 años. Gracias a las imágenes suministradas por el sistema de circuito cerrado de televisión la policía pudo aclarar el crimen, lo que generó entre la población una corriente de opinión favorable a estos sistemas de vigilancia.

El segundo acontecimiento muy posterior en el tiempo sucedió en 2005. Unos terroristas suicidas ejecutaron atentados simultáneos en varios vagones del metro y en un autobús en el centro de la capital de Inglaterra. 56 víctimas mortales y más de 700 heridos fue el resultado de esta masacre. La identidad de los terroristas se averiguó gracias a los documentos que llevaban consigo y a su ADN, pero tanto la ejecución de su actuación como su preparación fueron esclarecidos a través de las imágenes suministradas por las 2.500 cámaras situadas en el centro de Londres.

El Gobierno conservador de Jhon Major (1990-1997) informó que el Ministerio del interior dedicaría dos millones de libras para instalar sistemas de videovigilancia en los centros de las ciudades. En palabras de Michael Howard, en aquel momento Secretario de Estado: «La videovigilancia atrapa delincuentes. Reconoce los delitos, identifica los autores de los mismos y ayuda a enjuiciar a los culpables. La expansión de esta tecnología tiene como consecuencia que más centros de ciudades, zonas de compras, centros de tiendas y parques son un lugar prohibido para los criminales. […] Videovigilancia es un maravillosos complemento de la Policía»[13].

En la década que transcurre entre 1992 y 2002 el Gobierno Central a través del City Challenge Competition y de su programa para reducir la criminalidad invirtió cuantiosas sumas de dinero para la expansión de estos instrumentos de observación[14]. Hoy, en la mayoría de las ciudades británicas, si no en todas, sus centros están cubiertos por cámaras. No es fácil afirmar con

[13] Galdon Clavell, G., *Per què la videovigilancia? Seguretat, tecnologia i politiques urbanes* (tesis doctoral), 2012, p. 25. En http://www.tdx.cat/bitstream/handle/10803/96653/ggc1de1.pdf;jsessionid=28248FA32BD4F363864C560B2E9BF597.tdx2?sequence=1

[14] Squires, P., «Los sistemas de videovigilancia: lecciones útiles de una cultura útil de la vigilancia», *Ciudadanos, ciudades y videovigilancia. Hacia una utilización democrática y responsable de la videovigilancia*, p. 37. En http://cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Publication/CCTV_Publication_ES.pdf

precisión cuántas hay, aunque se sabe que el Centro de Gestión y de Control de la Policía puede tener acceso a 60.000. A título ilustrativo, solo en el aeropuerto londinense de Heathrow se pueden encontrar alrededor de 3.000.

Desde hace algún tiempo la videotécnica se está utilizando también para gestionar los grandes acontecimientos deportivos, sobre todo los partidos de fútbol, en donde ha demostrado ser una herramienta eficaz y estratégica para suprimir la violencia en los estadios y sus inmediaciones. El público británico se ha acostumbrado tanto a la utilización de estos instrumentos que a menudo son los propios ciudadanos los que reclaman su colocación.

En definitiva, en el Reino Unido la vigilancia a través de videocámaras, como se ha venido afirmando, encontró en los años noventa del siglo XX un terreno propicio para su expansión: un Ejecutivo que promocionaba su instalación con recursos financieros y organizativos; unos medios de comunicación partidarios y una opinión pública en general favorable; una tradición jurídica que desconocía el concepto de la esfera privada; y finalmente la necesidad de las administraciones locales de dar un nuevo impulso a los centros urbanos en declive como espacios comerciales atractivos y seguros para el consumidor[15]. Es importante señalar, sin embargo, que desde hace unos años, algunas voces se han alzado para cuestionar la pertinencia de la política de «videovigilancia total» y para extraer algunas conclusiones de la experiencia hasta ahora acumulada.

Los británicos están llevando a cabo una reflexión sobre sus sistemas y el modo de utilizarlos. El rápido despliegue de una tecnología aún poco contrastada hizo que se cometieran numerosos errores. La videovigilancia creció a gran velocidad en el entorno británico, bastante más de lo razonable si se tiene en cuenta la falta de pruebas de su eficacia o repercusión. Aparentemente su uso no parecía reducir demasiado los índices de criminalidad de las zonas en las que se había implantado. Sin embargo se crearon unas expectativas muy poco realistas impulsadas por una alianza integrada por entusiastas policías, agentes comerciales del sector de la seguridad y ciudadanos atemorizados. Estaban convencidos de que la videotécnica podía resolver muchos de los problemas de delincuencia y desorden a los que se tenían que enfrentar en los espacios públicos. Como se informó en un estudio del Ministerio del Interior británico llevado a cabo en el 2005: «Los sucesivos Gobiernos exageraron las bondades como respuesta ideal al problema del crimen. Pocos de los que deseaban hacerse con una porción de los fondos disponibles consideraron necesario demostrar la eficacia de la videovigilancia, y sin embargo, casi nunca estuvo del todo claro por qué ésta constituía la mejor arma para luchar contra el crimen en circunstancias particulares»[16].

[15] Arzoz Santisteban, X., *Videovigilancia, seguridad ciudadana y derechos fundamentales*, eds. IVAP, Civitas y Thomson Reuters, Pamplona, 2010, p. 24.

[16] Squires, P., «Los sistemas de videovigilancia: lecciones útiles de una cultura útil de la vigilancia», *op. cit*., p. 38.

Mike Neville, director de un departamento en Scotland Yard, realizó una critica severa los resultados conseguidos en Londres mediante estos sistemas de vigilancia calificándolos de «fiasco». A pesar de la intensa utilización de estos métodos, –1 cámara por cada 14 personas– sólo el 3% de los robos que se cometen en sus calles se esclarecen gracias a su ayuda[17]. El actual Viceprimer Ministro, Nick Clegg, anunció que el Gobierno preparará una nueva ley de protección de los derechos fundamentales. En una conferencia de prensa del 19 de mayo de 2010 declaró: «Este Gobierno pondrá un término a esta cultura de intrusión en la vida privada de sus ciudadanos. Es inaceptable que personas que respetan la ley sean tratadas como si tuvieran algo que esconder… La videovigilancia será objeto de leyes específicas…»[18].

Alemania, el país cuya regulación de la videovigilancia vamos a analizar en este trabajo, no fue tan precoz en el empleo de estas técnicas de reproducción de imagen ni tampoco ha experimentado una expansión tan rápida y creciente. La cultura tan arraigada existente de garantía de los derechos fundamentales, en general, y de tutela de los datos personales en particular, han impedido su crecimiento ilimitado, las amargas experiencias del pasado quizás hayan conducido a que la legislación alemana haya concedido una especial atención a la temática de la protección de datos. A lo largo de la historia las experiencias acumuladas por el pueblo germano con el empleo de las videocámaras con finalidad de seguridad pública han tenido naturaleza muy diferente.

Tanto bajo la dictadura del nacionalsocialismo como en la DDR, el uso de los aparatos de reproducción de sonido e imagen constituía una práctica común. El espionaje y la denuncia eran en los dos puntales en los que se apoyaba el poder[19]. De manera obsesiva los partidos y el Estado pugnaban por mantener el control sobre la población. En el ámbito público se utilizaban para vigilar a sus enemigos, es decir, a los periodistas del Este, a los defensores de los derechos, a los manifestantes y a todas las personas, en general, críticas con el régimen. Los sistemas de videocámaras eran odiados y temidos por una gran parte del pueblo alemán. Muchos ciudadanos no confiaban en poder hablar abierta y libremente en sus propias casas porque incluso allí eran espiados. Los más beligerantes con el Gobierno tenían pinchados sus teléfonos lo que suponía un atentado muy grave contra su privacidad. La película *La vida de los otros* ilustra de forma clara la situación sufrida en aquellos años en la RDA.

[17] Frentz, C., «Staatliche Videoüberwachung im Kreuzverhör», en *Forum*, nº 298, 2010, p. 7.

[18] Marcus, M., «El desafío: Conciliar el uso de la videovigilancia y las libertades individuales», *op. cit.,* p. 14.

[19] Masing, J., «Herausforderungen des Datenschutzes», en *Neue Juristische Wochenschrift*, nº 65, 2012, p. 2305.

Plazas, estaciones e importantes puntos del centro de la parte este de Berlín eran observados a través de numerosas cámaras. Desde mediados de 1989, el séptimo día de cada mes miles de personas se reunían en la *Alexanderplatz* para manifestarse en contra de la manipulación electoral. El material conseguido en este tipo de actos era muy útil para el Ministerio para la Seguridad pública (STASI) y para la Policía pues suministraba información imprescindible para sus archivos. Según la versión oficial el objetivo de las cámaras era el control del tráfico sin embargo la población en general sabía cuáles eran sus auténticos fines[20]. No es extraño por tanto que el empleo de las videocámaras en lugares de acceso público y privado tuviera en la Alemania del Este connotaciones tan negativas.

Estas mismas técnicas años más tarde eran empleadas con una finalidad completamente diferente. El 31 de julio de 2006 en los trenes regionales de Hamm y Koblenza se colocaron diversos artefactos que no llegaron a explotar. Estos hechos constituyeron un eslabón más de la cadena de atentados que se habían iniciado en Nueva York y se habían repetido en Europa en grandes capitales como Madrid o Londres. Gracias a la videovigilancia fueron identificados en Alemania en la estación de tren de Colonia los responsables de la instalación de las bombas. El éxito de las pesquisas policiales fue debido básicamente al análisis de las imágenes de vídeo. Por eso no puede extrañar que en las encuestas realizadas en agosto de ese mismo año, el 80% de los ciudadanos germanos se mostrasen favorables al incremento de estas medidas de vigilancia en trenes y autobuses frente a un 17% que expresaban su oposición. Recibían estos métodos el aplauso y respaldo de la mayoría de la opinión pública porque habían contribuido de forma notable al esclarecimiento de sucesos violentos muy graves[21].

La reacción de la población en general a la introducción de estas medidas es en líneas generales positiva. Existen sin embargo algunos reparos. Por un lado, se teme un abuso de la videotécnica por parte de los funcionarios, especialmente en la selección de los objetos videovigilados; o una discriminatoria, desproporcionada vigilancia de grupos marginales. Por otro lado, las crecientes posibilidades de observación técnica así como el almacenaje de datos y sus aplicaciones, generan una cierta inquietud entre los ciudadanos frente a un Estado vigilante o ante la aparición de lo que se conoce como personas de cristal (*gläsernen Menschen*)[22].

[20] Zilkens, M., «Videoüberwachung. Eine rechtliche Bestandsaufnahme», *Datenschutz und Datensicherheit*, nº 31, 2007, pp. 279-280.

[21] Abate, C., «Präventive und repressive Videoüberwachung öffentlicher Plätze», *Datenschutz und Datensicherheit*, nº 7, 2011, pp. 453-454. El autor en este artículo realiza una breve reflexión acerca de la utilidad de la videovigilancia como medio represivo y disuasor de la comisión de delitos en lugares públicos.

[22] La expresión personas de cristal (*gläsernen Menschen)* fue utilizada por primera vez en los años 20 para denominar el modelo anatómico humano elaborado en material de

3. EL OBJETO DE ESTUDIO

En este trabajo vamos a centrarnos en la regulación de la videovigilancia privada en lugares de acceso público en el derecho alemán desde la perspectiva del derecho a la protección de datos. Este país ha sido uno de los pioneros en la creación de un derecho fundamental a la autodeterminación informativa. Las amargas experiencias del pasado son probablemente la causa de que se haya otorgado una especial atención a este derecho[23]. Su contenido, en líneas generales, consiste en un poder de disposición y de control sobre los datos personales que habilita a la persona para decidir cuáles de ellos deben proporcionarse a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, permitiendo también al titular de los mismos saber quién los posee y para qué, pudiendo oponerse a esa posesión o uso. Estas facultades de disposición y control sobre los datos personales, constituyen el núcleo central del derecho fundamental y se concretan jurídicamente en la potestad de consentir la recogida, la obtención y el acceso a los mismos, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. 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 ellos y a qué uso los está sometiendo, y, por otro, el poder oponerse a esas dos operaciones**.**

La videovigilancia es el clásico ejemplo del conflicto entre la técnica de la vigilancia y el derecho a la autodeterminación informativa: los afectados no saben, quién y qué se esconde detrás de la cámara de observación.

Nos centraremos, pues, seguidamente en el análisis del § 6b BDSG (*Bundesdatenschutzgesetz*)[24] y la jurisprudencia que con motivo del mismo ha sido dictada por las diferentes instancias judiciales alemanas.

4. MARCO JURÍDICO EUROPEO DE LA VIDEOVIGILANCIA

Antes de adentrarnos en el examen del caso alemán conviene sin embargo, realizar una breve descripción de los principios fundamentales existentes a nivel europeo en el ámbito de la tutela de derechos y libertades fundamentales que afectan también –como no podía ser de otra manera– a la protección de datos de naturaleza personal, más concretamente los obtenidos a través de las operaciones de videovigilancia.

---

plástico transparente por el museo alemán de higiene. Desde hace algunos años este término se emplea sobre todo como metáfora de la protección de datos, sirve para denominar negativamente a las nuevas técnicas de observación así como al creciente interés de los Estados en obtener información sobre sus ciudadanos.

[23] MASING. J., «Herausforderungen des Datenschutzes», *Neue Juristische Wochenschrift,* nº 2305, 2012, p. 2306.

[24] Ley federal de protección de datos.

Con carácter general el Convenio europeo para la Protección de los Derechos humanos y Libertades fundamentales adoptó el Marco jurídico de la vídeovigilancia en Europa disponiendo en su artículo 8 el derecho a la intimidad de la vida privada y familiar, del domicilio y de la correspondencia[25].

El Convenio nº 108/1981 del Consejo de Europa sobre la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado por 40 Estados europeos (España entre ellos), constituye el primer instrumento internacional cuyo objetivo principal es sentar las normas mínimas para proteger a las personas de los abusos que pudieran producirse en este ámbito. Este Convenio se aplica por igual a los sectores público y privado y establece una serie de principios generales referidos a la recopilación, el tratamiento y la comunicación de datos de carácter personal por parte de las nuevas tecnologías de la información. Las actividades de videovigilancia entran dentro de su ámbito, en la medida en que implican el tratamiento de este tipo de datos, según lo define la Convención n° 108, y el Comité de Consulta que ha considerado que las voces y las imágenes deben concebirse como datos de carácter personal cuando suministran información sobre una persona facilitando su identificación incluso aunque sea indirectamente[26].

Las normas jurídicas que en él se contienen hacen hincapié en cuestiones de diversa naturaleza: el carácter lícito y leal de la recopilación y el tratamiento automatizado de los datos personales, las finalidades legítimas de la grabación y del registro, la limitación de la conservación de estas imágenes a un plazo estrictamente necesario, el carácter adecuado y no excesivo del sistema respecto a los objetivos que se persiguen, así como la pertinencia de los datos y la obligación de actualizarlos. El Convenio proscribe el tratamiento de datos «sensibles» (relativos a las características raciales, a las opiniones politicas, a la salud, a la religion, a la vida sexual), y garantiza, asimismo, el derecho que tienen las personas a conocer la información sobre ellas almacenada y de exigir, en su caso, las rectificaciones que sean precisas.

[25] Artículo 8 del Convenio europeo de derechos humanos: Derecho al respeto de la vida privada y familiar: «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituye una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o la moral o la protección de los derechos y libertades de los demás».

[26] Lim, L., «Marco jurídico de la videovigilancia en Europa», *Ciudadanos, ciudades y videovigilancia. Hacia una utilización democrática y responsable de la videovigilancia,* p. 90. En http://cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Publication/CCTV_Publication_ES.pdf

También el Tribunal europeo de Derechos humanos ha tenido la oportunidad de pronunciarse sobre los límites de las garantias en materia de videovigilancia. Así ha manifestado que la revelación y publicación en los medios de comunicación, en el marco de campañas de lucha contra el crimen, de imágenes obtenidas a través de sistemas de videovigilancia emplazados en la vía pública, y a espaldas de la persona filmada, violan el artículo 8.43 del Convenio.

En esta misma línea, con el afán de sentar un marco jurídico más específico para las operaciones de videovigilancia, y después de haber observado «con inquietud que las leyes nacionales están lejos de ser homogéneas en la materia», la Asamblea parlamentaria del Consejo de Europa adoptó el 25 de enero de 2008 la resolución n°1604. A través de ella se pide formalmente a los Estados miembros integrantes de este órgano europeo la aplicación conjunta de los «principios directivos para la protección de las personas respecto a la recopilación y el tratamiento de datos a través de la videovigilancia». Se trata de doce principios que retoman y trasladan a la videotécnica las directrices que los instrumentos del Consejo ha afirmado, insistiendo singularmente en las siguientes condiciones: una utilización pertinente, adecuada y no excesiva respecto a la finalidad que se persigue; evitar que los datos recopilados sean indexados, comparados y conservados sin necesidad; no efectuar una videovigilancia si el tratamiento de los mismos puede producir una discriminación contra algunos individuos o grupos de individuos, por razón de su opinión política, de sus convicciones religiosas, de su vida sexual, de sus caracteristicas raciales o étnicas; informar claramente y de forma adecuada a las personas indicando la finalidad del sistema y la identidad de los responsables; garantizar el ejercicio del derecho de consultar sus imágenes y grabaciones; y por último, proteger la seguridad e integridad de todos los afectados a través de toda medida técnica y organizativa necesaria[27].

Asimismo el Consejo de Europa anima a sus miembros a prever en su legislación nacional las disposiciones que definen las restricciones técnicas, destinadas a limitar la instalación de estos equipos en función del lugar que se deba vigilar y de las zonas privadas que se han de excluir del ámbito de la videovigilancia; exige la utilización de un *software* adecuado para la codificación criptográfica de los vídeos y la creación de vías de actuación jurídica en caso de que se alegue una utilización abusiva de estas técnicas de imagen. De igual manera la Asamblea parlamentaria considera necesario que se adopten lo antes posible una señalización y un texto de acompañamiento uniformes y que éstos sean utilizados por los Estados miembros y, en último lugar, destaca, la necesidad de continuar en el futuro con la reflexión sobre el tema de la videovigilancia a la vista de los progresos técnicos constantes que tienen lugar en este sector.

[27] Lim, L., «Marco jurídico de la videovigilancia en Europa», *op. cit.* (nota 26), p. 92.

Entre el resto de textos europeos dignos de ser citados aplicables a las actividades de videovigilancia hay que citar la Carta de Derechos fundamentales de la Unión europea. Esta proclamación solemne, adoptada el 7 de diciembre de 2000, ha sido mencionada en el Tratado de Lisboa de 13 de diciembre de 2007, en un precepto sobre los derechos fundamentales. El artículo 7 de la Carta dispone, primero, que «Toda persona tiene derecho a que se respete su vida privada y familiar, su domicilio y sus comunicaciones». A continuación, el artículo 8, garantiza el derecho a la protección de los datos de carácter personal que le incumben, indicando además, que deben ser tratados lealmente, con fines determinados, y sobre la base del consentimiento de la persona respectiva, o en virtud de otro fundamento legítimo previsto por la ley, estableciendo además el derecho de toda persona a consultar los datos registrados que le conciernen y a obtener su eventual rectificación, estando sometido el respeto de estas reglas al control por parte de una autoridad independiente.

Más concretamente es el Supervisor europeo de Protección de datos (CEPD), desde un posición independiente, quien se encarga de velar por el respeto de todas estas reglas, controlando los tratamientos de datos de carácter personal que llevan a cabo las instituciones europeas. Este órgano ha publicado el 17 de marzo de 2010 un conjunto de líneas directrices sobre la videovigilancia destinadas a las instituciones y organismos europeos en donde se incluyen una serie de recomendaciones prácticas. De hecho, destacan el concepto de *privacy by design*, según el cual las medidas técnicas de precaución que permiten proteger mejor los datos de caracter personal y la vida privada de las personas filmadas, deben estar incorporadas, desde la etapa inicial de diseño, en las características tecnológicas de los sistemas de vigilancia.

La Directiva 95/46/CE del Parlamento europeo y del Consejo europeo, del 24 de octubre de 1995, relativa a la protección de personas físicas respecto al tratamiento de los datos de carácter personal y a la libre circulación constituye el instrumento jurídico que ha hecho suyo la Unión europea para establecer sus principios de tutela. Sobre la base de este texto, los Estados miembros han elaborado sus respectivas legislaciones nacionales sobre tutela de datos. En principio, la Directiva incluye los sistemas de videovigilancia, dado que se aplica a toda información, comprendiendo aquélla en forma de sonido e imágenes, referida a una persona teniendo en cuenta todos los medios que pueden ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona con el fin de conseguir su identificación.

En efecto, las imágenes y sonidos atribuidos a personas físicas se consideran como datos de carácter personal, aún cuando las imágenes sean empleadas en el marco de la videovigilancia, e incluso si no están asociadas a los datos de identidad de la persona; en los casos que no correspondan a personas cuyo rostro ha sido filmado, y contenga otra clase de información

(por ejemplo, el número de la placa con la matrícula de su vehículo). Hay que señalar sin embargo que la videovigilancia de los lugares públicos solo parcialmente se contiene en la Directiva 95/46, en la medida en que no incluye el tratamiento de los datos en forma de sonidos y de imágenes, con una finalidad de seguridad pública, defensa, seguridad del Estado, para el ejercicio de sus funciones en el ámbito del derecho penal, o para otras tareas que no entren en el campo del derecho comunitario. Por lo demás, la Directiva no afecta al tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

A nivel europeo, el grupo de autoridades nacionales de protección de datos (conocido como «Grupo del Artículo 29» o «G29», o «GTA») ha precisado en una resolución de 2004[28] la interpretación de las disposiciones de la Directiva n° 95/46. Esta resolución destaca la necesidad de que las instituciones respectivas de los Estados miembros lleven a cabo una evaluación general de la videovigilancia para «evitar que una proliferación excesiva de los sistemas de adquisición de imágenes en lugares públicos y privados no implique una restricción injustificada de los derechos y libertades fundamentales de los ciudadanos», que tuviera como efecto volver a los ciudadanos «masivamente identificables en muchos lugares públicos y privados». También subraya la necesidad de acometer una valoración de la evolución de las técnicas de videovigilancia, con el fin de evitar que el desarrollo de *software* de reconocimiento del rostro de las personas y de la detección/previsión del comportamiento «no conlleve el paso masivo e inconsiderado hacia una vigilancia de tipo dinámico-preventiva»[29].

5. EL § 6B DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS

5.1. *Introducción*

En el año 2003 se incorpora a la Ley federal de Protección de datos (en adelante BDSG) el § 6b[30]. La utilización cada vez con mayor frecuencia de los sistemas de videotécnica en los lugares de acceso público hacía necesario un precepto como éste. Los instrumentos jurídicos privados de tutela de la propia imagen distribuidos por los diversos sectores del ordenamiento no establecían suficientes mecanismos para la defensa del derecho citado.

[28] Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara, adoptado el 11 de febrero de 2004.

[29] Lim, L., «Marco jurídico de la videovigilancia en Europa», *op. cit.* (nota 26), p. 95.

[30] Ley Federal Alemana sobre Protección de Datos o Bundesdatenschutzgesetz, de 27 de enero de 1977 (Bundesgesetzblatt,1977, I, p. 201) entró en vigor el 1 de enero de 1978. Fue modificada por primera vez el 20 de diciembre de 1990 (Bundesgesetzblatt, 1990, I, pp. 2954 y 2955) y entró en vigor el 1 de junio de 1991.

En el ámbito privado no se conocía ninguna regulación concreta sobre videovigilancia. Algunos aspectos aislados se contemplaban en el § 22f KUG (*Kunsturhebergesetzes*)[31] o Ley de Protección del patrimonio de 9 de enero de 1907. Las imágenes solo podían ser difundidas o hechas públicas si se contaba con la autorización de los que en ellas aparecían, excluyéndose únicamente de este régimen:

– Imágenes de la historia contemporánea.
– Imágenes en las que las personas son algo accesorio.
– Imágenes de reuniones o algo similar en las que se encontraban personas que hubieran participado. Y por último,
– imágenes con fines artísticos.

Los que vulnerando estas reglas difundían o difunden las imágenes –pues el precepto está aun vigente, ya que la KUG no ha sido derogada por el § 6b BDSG– serán según el § 24 KUG objeto de responsabilidad penal.

Los partidos políticos, las organizaciones económicas, la Administración pública, así como las asociaciones de ciudadanos y los responsables de este ámbito, insistían en la necesidad de incluir en la Ley federal de protección de datos un precepto como éste[32]. Su incorporación tras algunas vacilaciones iniciales tenía un doble objetivo: por un lado, adaptar, el derecho alemán al derecho europeo y por otro, ajustar la BDSG al avance y desarrollo técnico[33]. El 23 de mayo de 2001 entró en vigor.

El proceso de redacción del § 6b BDSG no estuvo exento de polémica. Se debatió de manera prolongada, si el apartado primero del precepto debía prever un minucioso catálogo de requisitos o si, por el contrario, era más oportuno que contuviera una regulación más genérica[34]. Finalmente el legislador optó por la incorporación de una norma abierta con la intención de que en el futuro y a la vista de la experiencia se procediese a su revisión, introduciendo las novedades adaptándola a la realidad práctica. En la actualidad, no obstante, la doctrina reivindica que sería conveniente una nueva Ley de Protección de datos debido básicamente a dos razones. Primero, a que las suce-

[31] Ley de protección del patrimonio, de 9 de septiembre de 1965 (*Bundesgesetzblatt*, 1965, I, p. 1273).

[32] Weichert, T., «Private Videoüberwachung un Datenschutzrecht», en *Detektiv-Kurier*, nº 4, 2001, p. 9.

[33] Bizer, J., «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen», en Spiros, S. (ed.), *Nomos Kommentar. Bundesdatenschutzgesetz*, 6ª edición, Nomos, Frankfurt am Main, 2006, pp. 583-585.

[34] Gola, P. Y Schomerus, R., «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen», *Bundesdatenschutzgesetz*, Rn 1-5, 10ª edición, 2010, München. En J:\Gola-Schomerus, BDSG § 6b Rn_ 1 - 5 - beck-online.mht. La abreviatura Rn hace referencia al margen del texto, que aparece numerado en muchas publicaciones alemanas.

sivas reformas han convertido a la BDSG en una norma muy poco clara para el público en general y de utilidad práctica escasa para los juristas. Segundo, a que la ley se ha quedado obsoleta y no se adecua en su conjunto a los avances de la técnica. La importancia creciente que ha cobrado Internet en los últimos tiempos en el campo del tratamiento de datos debería, según los expertos, reflejarse en el contenido de la norma ofreciendo respuestas acordes con los problemas que plantea esta nueva realidad. En este sentido la doctrina tiene muchas dudas acerca de si esta norma garantiza de forma eficiente los derechos de las personas afectadas por la videovigilancia[35]. Tras el análisis legal y jurisprudencial que efectuamos sobre este tema en el derecho alemán intentaremos responder esta cuestión.

5.2. *Regulación actual*

El § 6b de la BDSG queda redactado como sigue:

> «(Observación de lugares de acceso público mediante dispositivos óptico-electrónicos)
>
> (1) La observación de lugares de acceso público mediante dispositivos óptico-electrónicos (videovigilancia) únicamente será lícita si es necesaria
>
> 1. para el cumplimiento de funciones de entidades públicas,
> 2. para el ejercicio de las facultades de policía dentro de los edificios o
> 3. para la salvaguarda de intereses legítimos con fines concretamente establecidos y no existen elementos que permitan suponer que prevalecen intereses dignos de protección de los afectados.
>
> (2) La práctica de la observación y la entidad responsable habrán de hacerse reconocibles a través de medidas idóneas.
>
> (3) El tratamiento o utilización de datos recogidos mediante la observación a que se refiere el párrafo 1º serán lícitos si son necesarios para la finalidad prevista y no existen elementos que permitan suponer que prevalecen intereses dignos de protección del interesado. Los datos en cuestión únicamente podrán tratarse o utilizarse para fines distintos en tanto ello sea necesario para evitar peligros para la seguridad estatal y pública y para perseguir delitos.
>
> (4) En caso de que los datos recogidos mediante la videovigilancia se adscriban a una persona determinada, ésta habrá de ser informada sobre el tratamiento o la utilización de dichos datos con arreglo a lo establecido en los §§ 19 a y 33.

[35] WEDDE, P., «Videoüberwachung. § 6b», en DAÜBLER W., KLEBE, T., WEDDE, P., WEICHERT, T. (eds.), en *Bundesdatenschutzgesetz. Kompaktkommentar zum BDSG*, 3ª edición, p. 235.

(5) Los datos se cancelarán tan pronto como dejen de ser necesarios para la finalidad prevista o existan intereses dignos de protección del interesado contrarios a la conservación de la ulterior grabación»[36].

Las legislaciones de protección de datos de los diferentes Estados alemanes contienen normas de contenido muy similar[37] a la que aquí se transcribe a nivel federal, únicamente existen discrepancias menores en concretos aspectos de la regulación relativos, por ejemplo a la obligación de información[38] o a la autorización de almacenamiento de datos con finalidad de prueba[39].

5.3. *Ámbito de aplicación del § 6b BDSG*

5.3.1. Condiciones de la observación

El § 6b BDSG tiene por objeto la observación de lugares de acceso público a través de equipos ópticos-electrónicos tanto si se efectúa en los organismos públicos en el sentido expresado por los § 1 II nº 1 y nº 2 BDSG como en los no públicos en los términos del § 1 II nº 3 de la BDSG siendo su finalidad básica la de proteger los derechos de la personalidad de los afectados por la utilización de las videocámaras. Analizamos en consecuencia, en primer lugar, qué debe entenderse por observación; en segundo lugar, cuáles son los lugares de acceso público a que se refiere el precepto; y, por último, qué se incluye bajo la expresión de equipos ópticos electrónicos.

La videovigilancia puede ser definida como aquella actividad que tiene como principal finalidad la colocación de una videocámara, fija o móvil[40], para la vigilancia de un espacio o de personas.

El legislador utiliza en el apartado primero del precepto que ahora analizamos el término «beobachten», que puede ser traducido como observación. Esta actividad deberá realizarse durante un considerable período de tiempo porque la simple emisión de una imagen aislada mediante el empleo de estas cámaras de filmación no puede recibir esa calificación.

En la mayoría de las ocasiones la vigilancia a través de la videotécnica se efectúa por razones de seguridad aunque pudieran existir otros motivos,

[36] La traducción del § 6b de la BDSG al castellano es de la autora del artículo.

[37] Un precepto similar al § 6b de la BDSG podemos encontrarlo en las diferentes leyes de protección de datos de los *Länder*. Baviera (Art. 21a), Berlin (§ 31b), Brandenburgo (§ 33c), Bremen (§ 20b), Mecklenburgo-Pomerania Occidental (§ 37), Renania del Norte-Westfalia (§ 29b), Renania Palatinado (§ 34), Sarre (§ 34), Sajonia (§ 33), Sajonia-Anhalt (§ 30) y Schleswig-Holstein (§ 20).

[38] § 20 II de la Ley de Protección de Datos del *Land* Schleswig-Holstein.

[39] § 29b II de la Ley de Protección de Datos del *Land* Renania del Norte-Westfalia.

[40] Wedde, P., «Videoüberwachung. § 6b», *op. cit*. (nota 32), pág 238.

como por ejemplo, para satisfacción de la simple curiosidad, para efectuar un control laboral o simplemente con fines publicitarios, etc. En todo caso el legislador ha definido la videovigilancia en la BDSG como la observación de los lugares de acceso público con equipos ópticos electrónicos.

La norma distingue entre observación a la que alude en el apartado primero y la recogida en la forma de tratamiento o utilización a la que se refiere el apartado tercero. Un sector de la doctrina entiende que la observación sin almacenamiento de imágenes es suficiente para la aplicación del § 6b, tanto si se trata de una actuación pasiva como activa dirigida a un concreto fin u objetivo. Según los autores que se encuentran en esta línea de pensamiento es irrelevante para cumplir con el requisto de la observación si existe únicamente una intención por parte del autor de efectuar estas operaciones o si la recogida, el almacenamiento o la transmisión de las imágenes se materializan de forma efectiva. La norma no establece nada más al respecto, a diferencia por ejemplo de lo que sucede con el § 3 III BDSG que sí prevé esta distinción. En contra de esta opinión, un grupo de autores consideran que la obtención de datos personales es un requisito imprescindible para poder acudir al § 6b I BDSG y de hecho existe una remisión a lo previsto en el § 1 II nº 3 BDSG[41].

En ningún caso puede la observación focalizarse en una persona concreta, aunque sí se permite por parte de la norma que el lugar público sea filmado de manera que posibilite la identificación de las personas que allí se encuentren, pues de no ser así, la videovigilancia no tendría sentido. Lo que, por otro lado, sí se establece a nivel legal es la obligación de emplear técnicas que posibiliten, tal y como establece el § 3 BDSG, el anonimato. El diseño y la selección de los sistemas de tratamiento de datos deberá efectuarse teniendo en cuenta los principios de no recogida, tratamiento o utilización de datos personales o si es preciso hacerlo con el menor número de ellos posible. En particular se recurrirá a anonimizar y a pseudoanonimizar en la medida en que ello sea necesario y el despliegue de medios sea proporcional a la finalidad protectora prevista.

5.3.2. Lugar público

El § 6b BDSG permite la videovigilancia de lugares públicos. Pero, ¿qué debe entenderse a estos efectos?

El término «lugar público»[42] no ha sido definido de manera general en el derecho alemán, variando su significado dependiendo de la rama del derecho de que se trate.

---

[41] Lang, M., *Private Videoüberwachung im öffentlichen Raum*, Dr. Kovač, Hamburg, 2008, p. 272.

[42] Huff, M. W., «Videoüberwachung im öffentlichen und privaten Bereich. Eine Zwischenbilanz», *Jus*, nº 10, 2005, p. 897.

Con carácter general, lugar público es el espacio al que cualquier persona tiene derecho a acceder y derecho a utilizar, en contraposición con los privados, en los cuales su entrada está restringida, generalmente por criterios de propiedad privada, reserva estatal, etc. Resulta irrelevante si se trata de un local abierto o cerrado, o si el propietario es un particular o un ente público. Son, por ejemplo y sin ánimo de exhaustividad, lugares públicos, las calles, las plazas, las zonas de paseo, las gasolineras, los negocios, los supermercados, las galerías comerciales, los restaurantes, los internets-cafés, los bancos, las piscinas y bibliotecas, así como las estaciones de tren o de metro. Su naturaleza pública no varía si para poder acceder a ellos es preciso cumplir con ciertos requisitos, como puede ser alcanzar la mayoría de edad o respetar un determinado horario de apertura.

La calificación de los accesos a los edificios de viviendas varía dependiendo de las circunstancias del caso. En principio, como únicamente sus habitantes y visitantes disfrutan del correspondiente derecho de entrada y salida, se calificarían como privados. Por el contrario, si se encuentran formando parte de un camino de acceso público y no dentro de uno de tránsito limitado, tendrían naturaleza pública.

Las escaleras de las casas y las entradas de los edificios de utilización mixta, es decir, los que se sitúan en viviendas privadas y locales de uso público, se incluyen dentro de los lugares de acceso público. Comparten esta misma categoría las consultas médicas, los bufetes de abogados, los salones de estética o los negocios, aunque en todos ellos el carácter público quedaría limitado a los horarios de consulta o de apertura de los mismos, al igual que sucede con los centros comerciales, los negocios o los bancos[43].

Los espacios en los que para acceder se requiere la compra de un billete o una entrada también tienen la consideración de públicos, por ejemplo, los teatros, los casinos, los cines, los museos, los estadios de fútbol, los parques de atracciones, etc. en contraposición a las viviendas, los complejos residenciales, los jardines privados, los recintos empresariales, las oficinas, los locales de empresas, etc. Todos ellos son de carácter privado[44].

Existen un conjunto de lugares díficiles de clasificar como privados o públicos a los efectos de la instalación de la videovigilancia. Ni el texto de la BDSG ni tampoco la justificación contenida en su proyecto contribuyen a esclarecer la naturaleza de los mismos. Estaríamos hablando, por ejemplo, de las zonas en las que se encuentran los cajeros de los bancos y las cajas de ahorro a las que únicamente se puede acceder fuera del horario laboral a través de una tarjeta de crédito o de cliente[45].

[43] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), p. 15.
[44] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), p. 16.
[45] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), p. 242.

Especialmente problemático resulta también el tratamiento de aquellas superficies en donde los empleados están afectados por la videovigilancia de lugar público, como ocurre, por ejemplo, con las gasolineras, las tiendas, las estaciones o las salas de juego. De acuerdo con lo que establece la BDSG, los lugares de trabajo no entran dentro del ámbito de aplicación de esta ley ni tampoco los datos de los trabajadores. Sin embargo, es cierto también que si en estos emplazamientos concurre al mismo tiempo la característica de locales de acceso público hay que aplicarles el § 6b I BDSG, de manera continuada o bien de forma temporal vinculándolo al horario de apertura al público. La situación puede complicarse todavía más si dentro de un mismo local o lugar de trabajo es preciso, a su vez, hacer distinciones o diferenciaciones de régimen. Si a a los espacios únicamente puede acceder el personal y no los clientes como ocurre con los habitáculos en los que se encuentran las cajas, las cabinas o los mostradores, no puede aplicárseles lo dispuesto en el § 6b BDSG. Pero si se trata de estancias abiertas al público, en donde la videovigilancia alcanza tanto a los empleados como a los clientes, como acontece por ejemplo, con el salón de una cafetería, les afectaría este régimen. No debe planificarse para ellos una total vigilancia sino que el empresario tendrá que preocuparse por la instalación de un sistema que restrinja lo menos posible los derechos de la personalidad de sus empleados. En casos aislados incluso los servicios de videotécnica podrían ser sustituidos por vigilantes que desarrollasen esta función[46].

Si el lugar de trabajo no es de acceso público no se aplica de ninguna forma el precepto que estamos examinando. La intensidad de la injerencia provocada por la videovigilancia cuando nos encontramos con espacios de estas características es mucho mayor que si estamos ante un lugar de acceso público. El círculo de personas vigiladas en los puestos de trabajo no es anónimo sino todo lo contrario, previsible y conocido por el empresario que decide la colocación de estas cámaras. La presión que se ejerce sobre los trabajadores a través estos sistemas es muy superior a la recibida por el público en general en otros espacios públicos como son las gasolineras, los centros comerciales, los transportes públicos, etc. En estos últimos la observación suele ser superficial y por un corto espacio de tiempo. Por el contrario, en el local de trabajo la observación dura más horas y potencialmente se repite cada día sin olvidar además que el trabajador no puede evitar la estancia vigilada ni tampoco dispone de la posibilidad de alejarse de ella[47].

El autor de la BDSG en su exposición de motivos advierte que sería conveniente que una ley específica de protección de datos de los trabajadores

[46] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), pp. 242-243.

[47] Wedde, P., «Videoüberwachung. § 6b», *op. cit.* (nota 35), p. 239.

contemplase un precepto similar al § 6b. Hoy, transcurridos doce años esta ley, todavía no ha sido aprobada.

5.3.3. Equipos ópticos electrónicos

Por último la norma examinada dispone que la observación se realizará a través de equipos ópticos-electrónicos. La característica fundamental de estos aparatos es que transforman la luz en una señal eléctrica, razón por la cual se incluyen aquí todo tipo de cámaras y equipamientos electrónicos que pudieran ser utilizadas con fines de observación[48]. La norma afecta principalmente a las videocámaras y a las cámaras *webs*, pero también a los móviles cuando en los lugares públicos se toman imágenes y se transmiten o los *iphone* con los que se graban videos y despúes se cuelgan en plataformas de Internet, como por ejemplo *you tube*[49].

Con el término «videovigilancia» se hace referencia a una amplia gama de sistemas a través de cámaras con soluciones técnicas diferentes y que están en permanente desarrollo. Las videocrámaras están básicamente integradas, por un elemento de captación de la imagen (por ejemplo, una cámara), uno de visualización (por ejemplo, una pantalla) y uno de almacenamiento (por ejemplo, un disco duro). Para que lo registrado sea utilizada de forma inmediata o en un momento posterior, debe ser transmitido al elemento de visualización o al de almacenamiento respectivamente.

Es indiferente para el derecho de protección de datos que las videocámaras sean análogicas o digitales. En un principio no estaba muy claro, como consecuencia de la anacrónica regulación en la BSDG, si las imágenes y las copias podían ser clasificadas como datos si no eran digitales, pues se entendía que esta característica constituía un requisito imprescindible para la aplicación del régimen de la protección de datos. En la actualidad el término datos se maneja en sentido amplio, quedando comprendido dentro de él toda información sobre aspectos personales o elementos objetivos de una persona física identificada o identificable (el interesado) incluyéndose, por tanto, aquí también los ficheros no automatizados[50]. Igualmente resulta irrelevante para la aplicación del precepto si se trata de una cámara fija o móvil o cuál es la técnica por ésta empleada (*zomm*, posibilidad de valoración, forma de almacenamiento, en red, etc.).

No existe en la literatura jurídica germana ningún acuerdo acerca de qué aparatos junto con las videocámaras deben ser catalogados como equipamientos óptico-electrónicos. Para unos autores forman parte de este grupo

[48] Wedde, P., «Videoüberwachung. § 6b», *op. cit.* (nota 35), p. 239.

[49] Wedde, P., «Videoüberwachung. § 6b», *op. cit.* (nota 35), p. 238.

[50] Weichert, T., «Private Videoüberwachung und Datenschutzrecht», *op. cit.* (nota 32), p. 10.

las videocámaras y *webcams* pero no otras cámaras como prismáticos o cámaras de fotos que disponen también de funciones electrónicas. Sin embargo otro sector doctrinal sostiene que dentro de este grupo se ha de incluir cualquier aparato siempre que sea apto para realizar una función electrónica[51].

En este contexto nos planteamos si las cámaras de imitación, también denominadas *dummys,* entrarían dentro del círculo de aplicación de la norma en cuestión. Estos aparatos no se basan ni en el procedimiento óptico-electrónico ni permiten realizar una observación con el sentido y finalidad que el § 6b BDSG exige por lo tanto lo más lógico es que sean excluidos[52].

Las diversas modalidades técnicas de videovigilancia han sido ordenadas de menor a mayor, atendiendo al grado de injerencia en los derechos fundamentales del siguiente modo:

– en la posición inferior de la tabla estaría la simple observación física de un espacio por una persona que controla uno o varios monitores,
– a continuación, se encontraría la observación con grabación simultánea de imágenes panorámicas;
– el siguiente lugar en la tabla lo ocuparían los sistemas que permiten la individualización de las personas contempladas a través del *zoom* de pantalla o la ampliación posterior de la imagen;
– por último, encontraríamos los sistemas inteligentes de videovigilancia cuya misión es el reconocimiento facial de la voz o la matrícula de los vehículos e incluso un seguimiento del sospechoso por un área relativamente extensa[53].

La BDSG no resuelve con la claridad necesaria si las restricciones previstas en el § 1 II nº 3 BDSG son aplicables a los entes no públicos y en caso de que lo fueran, en qué medida.

---

[51] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), pp. 246-247.

[52] Los autores discuten acerca de si el precepto es de aplicación a las cámaras de imitación. Los partidarios de su inclusión sostienen que en la definición contenida en la BDSG no se hace referencia a la idoneidad del aparato electrónico para realizar la videovigilancia mientras que en la BAG si se alude a ello de modo expreso. Según esta norma el aparato de videovigilancia es un equipamiento técnico que posibilita el control del comportamento y el rendimento de los trabajadores. Seifer, B., «Videoüberwachung im künftigen Beschäftigtendatenschutzrecht», *Datenschutz und Datensicherheit*, n° 2, 2011, p. 101.

[53] Arzov Santisteban, X., «Videovigilancia y libertades», en Etxebarria Guridi, E Y Ordeñana Gezuraga, I. (coordinadores), *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales*, Tirant lo blanch, Valencia, 2011, p. 156.

5.3.4. *Supuestos excluidos*

La BDSG prevé dos supuestos de videovigilancia de lugares de acceso público que quedan excluidos del régimen general previsto en el § 6b incluido en el Capítulo titulado «Disposiciones generales y comunes». Se trata en primer lugar de los sistemas de videotécnica instalados y utilizados por agencias y empresas con finalidad periodística y en segundo lugar de los desarrollados como actividad exclusivamente privada o familiar.

Por lo que se refiere a los primeros, el § 41 de la Ley contiene una reglamentación especial para ellos. Los Estados federados habrán de establecer en su legislación que cuando la recogida, tratamiento y utilización de datos personales sea efectuada por empresas o auxiliares del sector periodístico con fines exclusivamente periodísticos y redaccionales o literarios, se aplicarán disposiciones acordes con lo establecido en parágrafos propios de la Ley, incluyendo una disposición en materia de responsabilidad referida a las mismas.

Si la recogida, el tratamiento o la utilización de datos personales con carácter periodístico y redaccional tiene como responsable a la *Deutsche Welle* (Canal alemán)[54] e implica la publicación de réplicas o rectificaciones, éstas se unirán a los datos registrados y se conservarán por el mismo espacio de tiempo que dichos datos.

Si un reportaje de la mencionada cadena de radio y televisión supone una intromisión en los derechos de la personalidad, la persona afectada podrá exigir que se le informe sobre los datos registrados que hayan servido de base a la investigación en cuestión. La información podrá denegarse previa ponderación de los intereses en juego únicamente en dos supuestos. Primero, si los datos permiten identificar a personas que participen o hayan participado profesionalmente como periodistas en la elaboración, producción o difusión de emisiones de radioteledifusión; o al remitente o responsable de servicios, documentos o comunicaciones para la parte redaccional. Y segundo, si el suministro de los datos investigados u obtenidos de otro modo perjudicaría la función periodística de la *Deutsche Welle* por la exploración del material informativo disponible.

El segundo supuesto que queda fuera del ámbito de aplicación del § 6b BDSG es la videovigilancia desarrollada como actividad exclusivamente privada o familiar. En estos casos es preciso examinar para valorar la finalidad de la observación y de la grabación las circunstancias en las que se produce. Si de acuerdo con lo que dispone el § 1 II n° 3 BDSG estas actividadades tienen una naturaleza exclusivamente privada o familiar quedarían excluidas del régimen común mientras que si su dedicación fuera sólo parcial[55] se regirían por el mismo.

[54] En el § 41 BDSG se contiene una referencia específica a la Deutsche Welle.

[55] El § 1 II nº 3 de la BDSG emplea el término «ausschlieβlich» que significa exclusivamente, de ahí que la doctrina interprete que si la dedicación a las actividades privadas

Tanto si se trata de grabaciones con fines familiares como privados las cámaras deberán limitarse a operar en los lugares donde se desarrollan estas actividades. En consecuencia no tiene entrada aquí el § 6b BDSG que se prevé expresamente para «lugares de acceso público» en donde estos sistemas de vigilancia se instalan en la mayoría de los supuestos por razones de seguridad, bien para disuadir a posibles delincuentes de la comisión de delitos o bien para conservar las pruebas en los casos de comisión de algún acto o hecho ilícito[56].

La filmación de un lugar de acceso público para obtener pruebas de un comportamiento no ajustado a derecho de un tercero con la intención de proteger la posterior persecución jurídica del mismo sobrepasa el ámbito de las actividades exclusivamente privadas y familiares. Con el aseguramiento de la prueba se persigue retener a una persona que normalmente no pertenece al círculo privado o familiar para el caso de que se plantee una denuncia o una reclamación civil ya sea por los afectados o bien de las correspondientes instituciones. La tutela de las pruebas se encuentra fuera las actividades privadas o familiares y forma parte del ámbito del § 6b de la BDSG[57].

6. LICITUD DE LA OBSERVACIÓN

Como antes señalábamos, el § 6b I BDSG regula únicamente la videovigilancia u observación de lugares de acceso público mediante dispositivos ópticos electrónicos, actividad ésta que debe ser diferenciada del tratamiento, almacenamiento, transmisión así como de la utilización de los datos personales. Los requisitos legales de estas operaciones están previstos en el mismo parágrafo de la BDSG, pero en otros apartados (III, IV y V), a los que nos referiremos en otro lugar de este trabajo.

Lo que ahora en concreto vamos a examinar, es el § 6b II BDSG, en él se describen tres diferentes supuestos en los cuales la videovigilancia privada en lugar de acceso público es considerada conforme a derecho.

El primero se refiere a su establecimiento para el cumplimiento de funciones de las entidades públicas; el segundo, cuando tiene como finalidad el ejercicio de facultades de policía dentro de los edificios (o para garantizar el *Hausrecht*); y en último y tercer lugar, su objetivo consiste en salvaguardar intereses legítimos cuyos fines han de ser establecidos de manera específica.

---

y familiares se hace sólo parcialmente resulte de aplicación el § 6b de la BDSG. Bizer, J., «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen», *op. cit*., p. 588.

[56] Bizer, J., «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen», *op. cit.* (nota 55), p. 588.

[57] Bizer, J., «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen»», *op. cit.* (nota 55), p. 589.

En el primer caso el legislador entiende que la observación es lícita siempre que sea para cumplir con las tareas que les son encomendadas a los organismos públicos y que serían las que se deducen de lo previsto en la Constitución, las leyes, los reglamentos y el resto de las normas jurídicas. La función no tiene que ser satisfecha por completo a través del recurso a estos medios técnicos sino que es suficiente con que represente una contribución o colaboración a su ejecución. Este supuesto está pensado para garantizar, por un lado, la seguridad de las autoridades federales y por otro, para tutelar la conservación de las instalaciones y obras públicas, por ejemplo, para la vigilancia de diques y puentes con objetivos de seguridad o incluso evitar posibles catástrofes. A nivel estatal, los *Länder* disponen de normas similares para los entes públicos que han sido aprobadas en ocasiones con anterioridad a la norma federal, sin embargo, ni en este ámbito ni a nivel estatal existe un precepto equivalente para los entes no públicos. Este trabajo tiene por objeto el análisis de la videovigilancia privada en lugares de acceso público por lo tanto no vamos a detenernos más en el examen de este primer supuesto.

El segundo objetivo lícito que pueder perseguirse con la videovigilancia, es la salvaguarda del *Hausrecht*[58], que podría traducirse como el ejercicio de las facultades de policía dentro de los edificios, bien por parte de los propietarios o bien por los responsables de los mismos y que aquí, a diferencia de lo que ocurría con el caso anterior, se prevé tanto para los organismos públicos como para los no públicos[59].

El derecho de policía en el ámbito del derecho público se regula por normas de derecho administrativo aunque su contenido no es diferente al que pueda tener en el ámbito civil o penal. Se podría definir como la facultad que le corresponde al propietario o responsable de un recinto de decidir quién puede acceder a él y a quien es posible expulsar para mantener el orden dentro del mismo. La titularidad de este derecho corresponde a una o varias personas y permite a las que la ostentan adoptar todas las medidas que consideren oportunas para la tutela tanto del lugar como de las personas que en su interior se encuentran así como también de efectuar lo necesario para impedir el acceso de las no autorizadas. Su ámbito de protección comprende el interior y exterior de los edificios incluyendo los lugares de acceso a los mismos e incluso también a los vehículos.

La finalidad con la que se implementa la videovigilancia en estos casos tiene una doble naturaleza. Por un lado, preventiva, dirigida a evitar la comisión de cualquier delito como puede ser el de robo, hurto, daño en las cosas

[58] Sobre el *Hausrecht* vid.: ZIEGLER, J., «Das Hausrecht als Rechtsfertigung einer Videoüberwachung», *Datenschutz und Datensicherheit*, nº 27, 2003, pp. 337-340.

[59] GOLA, P. Y SCHOMERUS, R., «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen», *op. cit.*, Rn 16. En J:\Gola-Schomerus, BDSG § 6b Rn_ 14 - 18 - beck-online.mht.

o la realización de posibles destrozos en viviendas, negocios, etc. Por otro lado, represiva, orientada a la obtención de pruebas para perseguir e incriminar a los autores de los delitos. Por ejemplo, en los supuestos en que las videocámaras se instalan en un banco o en un aparcamiento no sólo tienen el efecto disuasor frente al delito sino también garantizador del material de prueba para el caso de que se produzca una tentativa o se llegue a cometer el hecho delictivo. No cabe duda de que en algunas ocasiones la presencia de videovigilancia en estos lugares favorece más que perjudica a las víctimas de los hechos ilícitos sobre todo cuando las imágenes obtenidas por las cámaras son almacenadas. Los mismos efectos beneficiosos producen estos sistemas en los cajeros automáticos en los que en muchas ocasiones se utilizan tarjetas de crédito falsas o se llevan a cabo atracos. La práctica demuestra que estos sistemas técnicos han sido efectivos en todos estos lugares. Ahora bien su colocación deberá realizarse de la forma que menos limite o restrinja los derechos de los afectados. Sería ilícito, como así consideró el Tribunal superior de Berlín en una sentencia de 26 de junio de 2002, un sistema de videocámaras que permitiera a los habitantes del edificio poder controlar a los visitantes a través de la presencia de monitores en las viviendas[60].

La doctrina parte de la afirmación de que la ubicación de videovigilancia es legal siempre que no vaya más allá de los límites espaciales del *Hausrecht*. En consecuencia no debería invocarse este derecho para grabar mediante cámaras objetos o locales que se encuentran emplazados en lugares colindantes a un camino público. Los autores distinguen aquí entre el ámbito local de tutela del derecho que finaliza en la propia finca y el alcance espacial de las acciones lícitas para su defensa. En la mayoría de las ocasiones es al titular de la finca al que le corresponde fijar la extensión de la videotécnica más allá de los límites de su terreno. Se trata sobre todo de una cuestión de necesidad y de adecuación de la medida adoptada para garantizar el derecho. Este derecho de morada o *Hausrecht* ampara, por ejemplo, la vigilancia frente a posibles daños en un lugar de acceso o en la pared de una casa que se sitúa en los lindes de un terreno público. Pero no sucede lo mismo si se quisisiera captar la imagen de visitantes no deseados en terrenos colindantes con los límites de un camino público. Esa finalidad no está protegida por el derecho invocado[61].

Con anterioridad a la entrada en vigor del § 6b BDSG, el Tribunal supremo alemán manifestó en alguna de sus sentencias que el *Hausrecht* solo en casos extremos permite al ocupante de una vivienda que necesite defenderse frente a injerencias que sufre del exterior, la observación de un camino y la grabación de imágenes de los que por él circulan. Los ataques a los derechos

[60] *Datenschutz und Datensicherheit*, nº 2002, p. 633.

[61] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), pp. 285-286. Bizer, J., «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen», *op. cit.* (nota 35), p. 592.

de la personalidad han de ser justificados en cada caso concreto siendo necesario realizar una valoración atendiendo a las circunstancias y a los intereses en juego de las partes implicadas en el asunto. Según el Tribunal, la grabación de imágenes puede ser legal si se producen graves ataques en los derechos de los responsables o en la esfera inmediata de la vivienda y no existe ningún otro medio para proceder a su reparación. Si las circunstancias son otras no existe en opinión del juzgador ningún motivo para obligar a que los que circulan por un camino de acceso público tengan que soportar que capten su imagen lo que constituye una manifestación concreta de sus derechos de la personalidad[62].

A partir de la promulgación del § 6b BDSG, la jurisprudencia del Tribunal supremo experimentó un cambio notable con respecto al tratamiento jurídico de los lugares de acceso público mostrándose mucho más permisiva con los sistemas de videovigilancia . Recientemente se ha pronunciado este Tribunal en una sentencia de 8 de abril de 2011 acerca de la implementación de unas cámaras en la entrada de una vivienda. Se activaban automáticamente cada vez que sonaba el timbre, transmitían una imagen con una duración de aproximadamente un minuto sin producirse ningún almacenamiento posterior. El Supremo consideró conforme a derecho la colocación de la cámara en este espacio de acceso público, porque tenía como objetivo salvaguardar el *Hausrecht* del propietario y no existía otro medio técnico menos invasivo con los derechos de los viandantes para lograrlo. No apreció tampoco la existencia de otros intereses preponderantes que debían ser tomados en consideración. Las imágenes obtenidas se utilizaban de manera temporalmente limitada y restringida, únicamente para que el propietario pudiera identificar a los visitantes de la casa y así poder autorizar o impedir su entrada. Por otro lado, la posibilidad de que el sistema de vídeo pudiera ser manipulado por un experto para conseguir, como afirmaban los demandantes, una vigilancia permanente o continua, no podía considerarse, en opinión del Tribunal, como constitutivo de extorsión o perjuicio para los derechos de los afectados[63].

En la práctica, los sistemas de videovigilancia que se encuentran en los locales de negocio no se colocan por los propietarios ni por los titulares de la explotación sino por los servicios de seguridad privada. La responsabilidad desde el punto de vista de la protección de datos tras la firma del correspondiente contrato es asumida por la empresa de vigilancia que será la encargada del tratamiento de los mismos. El régimen jurídico en estos casos es, por tanto, completamente diferente a cuando existe una delegación por parte del

[62] HOEREN, T., *Videoüberwachung und Rechte. Grenzen der Videoüberwachung im privaten und öffentlichen Raum,* Stuttgart, 2010, p. 8. En htp: www.stiftungaktuell.de

[63] En http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=10e3cc86e4da38d781acf2fe545c7569&nr=56316&pos=2&anz=

titular del negocio hacia la empresa de seguridad, en donde, según el § 11 BDSG, es el dueño del negocio el que permanece como responsable[64].

La tercera causa que justifica el empleo de las cámaras de grabación es la salvaguarda de intereses legítimos de fines específicamente previstos y se orienta fundamentalmente a los organismos no públicos.

La expresión utilizada en el § 6b III BDSG «salvaguardar los intereses legítimos» ha sido objeto de duras críticas por parte de la doctrina que la ha calificado como innecesariamente amplia. En ella se encuentran comprendidas desde un punto de vista general todas las finalidades jurídicamente admisibles que deben ser interpretadas de conformidad con la Constitución pues todas las injerencias en los derechos fundamentales han de ser legítimas. El legislador consciente de que la expresión empleada era demasiado genérica intentó corregirla disponiendo que los fines tienen que ser descritos de manera concreta. Sin embargo, al no haberse regulado el cuándo, el dónde y a quién le corresponde la verificación de estos objetivos, la indeterminación existente no fue eliminada[65].

El establecimiento de este requisito –de especificación de los fines– no permite resolver el problema porque con su inclusión no se está limitando el amplio abanico de finalidades ni tampoco su posterior determinación. De lo que no cabe duda es de que mientras que la previsión de los fines de la videovigilancia sea una tarea que se le encomiende al organismo responsable de su implementación (empresa de seguridad o titular del espacio o local de acceso público) y no a una tercera entidad independiente el problema se mantiene. Si, por el contrario, se hubiera introducido una obligación de comunicación de esta actividad a una autoridad de control tendría que ser ésta la encargada de examinar la plausibilidad de los fines y no existiría, en consecuencia, la posibilidad de cambiarlos discrecionalmente por el responsable de la videovigilancia, como en mayoría de las ocasiones viene sucediendo en la práctica[66].

Según adelantábamos en otro lugar de este trabajo, en la vida cotidiana la mayoría de las cámaras se colocan por motivos de seguridad pero pudiera hacerse por otras causas como por ejemplo para efectuar un control laboral. Como principio general el emplazamiento en estos espacios de cámaras ocultas es ilegal. El establecimiento de videocámaras de forma secreta pudiera ser legal si el empresario tiene sospechas fundadas de que alguno de sus trabajadores está realizando actuaciones ilícitas y se han agotado los otros medios disponibles menos lesivos con los derechos de la personalidad

[64] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), p. 286.

[65] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), pp. 287-288.

[66] *Begründung zur Beschlussempfhelung des Innenausschusses, BT-Drs*, 14/5793, p. 61. En http://dip21.bundestag.de/dip21/btd/14/057/1405793.pdf

para averiguar lo sucedido. En este caso el carácter inevitable de la videovigilancia la convierte en una medida lícita de investigación como así lo ha manifestado el Tribunal laboral de Friburgo en una sentencia de 7 de diciembre de 2004[67].

En cualquier caso, la necesidad de tener que recurrir a la videotécnica debe justificarse de forma objetiva sin poder atenderse exclusivamente al interés subjetivo del organismo responsable de su implementación. Los requisitos de cumplimiento no son muy estrictos, sino que basta para poder emplazar las cámaras de seguridad con la existencia de una situación de peligro abstracto que deberá ser fácilmente demostrable en situaciones que según la experiencia son típicamente arriesgadas[68].

La exigencia de probar el peligro no impide lógicamente ni a los dueños ni tampoco a los responsables de la gestión de un centro comercial o supermercado recién construido, invocando el § 6b I n° 3 BDSG, instalar cámaras de vídeo con la finalidad de evitar –si los actos ilícitos no han sido perpetrados– y perseguir delitos patrimoniales. Como la experiencia enseña que en estos lugares con frecuencia se cometen infracciones no se exige ninguna otra prueba adicional. Lo mismo ocurre en aquellos casos en que los sistemas de videovigilancia se colocan en edificios para evitar destrozos provocados por grafiteros. No es necesario que los propietarios de las casas o sus vecinos hayan sido víctimas de este tipo de actuaciones sino que basta únicamente con que exista una alta probabilidad de que puedan producirse. Lugares potencialmente amenazados por delitos como los de hurto, robo o daño en las cosas, se encuentran, por ejemplo, en los cajeros automáticos, en las cajas de seguridad situadas en las estaciones de tren, en los andenes y en los espacios exteriores de algunos edificios. También en los centros comerciales, en los supermercados alejados de lugares transitables o en los negocios difícilmente visibles así como en los accesos a grandes tiendas, a las casas de viviendas o a las parcelas aparecen estos escenarios de riesgo[69].

Las cámaras pueden introducirse para perseguir otros objetivos diferentes a los de seguridad. Lo que ocurre es que en muchas ocasiones estos motivos no tienen entidad suficiente para justificar el recurso a la videotécnica. Por ejemplo, razones comerciales no bastan por sí mismas, no son apropiadas, ni suficientes para permitir el empleo de la videovigilancia y en consecuencia para provocar una intromisión en los derechos de la personalidad de posibles afectados. Si una empresa quiere utilizar con fines publicitarios imágenes de sus locales de venta o de otros espacios de acceso público, como puede ser la

[67] *Bundesdatenschutzgesetz*. 41 Lieferung der Gesamtdokumentation, Juli, 2006, págs 1-4.

[68] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), p. 289.

[69] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), pp. 289-290.

parte frontal de sus escaparates o la sala de una discoteca, deberá proteger el derecho a la intimidad de las personas que allí se encuentran –si no han dado su consentimiento para la distribución de su imagen– a través del empleo de tecnología que no impiden su identificación.

Especialmente problemático en la práctica es el empleo de videocámaras en lugares de acceso público, por diversión, como *hobby* o por satisfacción simplemente de la curiosidad. Todas estas razones podrían ser catalogadas como intereses no lucrativos y por sí mismos no bastarían para justificar las injerencias en el derecho a la autodeterminación informativa de los posibles afectados que se pudieran derivar del empleo de la videotécnica en estos casos.

La videovigilancia a tenor de lo previsto en el § 6b I nº 3 será lícita cuando con carácter previo a su puesta en funcionamiento se describan los fines de la misma y éstos no se vean modificados con posterioridad. El empleo de expresiones de carácter general como *Gefahrenabwehr* (defensa frente al peligro) o *Verfolgung von Straβtat*e (persecución de los delitos) para expresar los objetivos perseguidos con la instalación de las cámaras no se consideran, conforme a derecho por ser demasiado genéricas. Los fines no tienen que ser formulados por escrito sino que puede hacerse de formas diferente[70] pues el § 28 I nº 2 BDSG así lo posibilita. En cualquier caso la voluntad del legislador es clara: la forma empleada para determinar los objetivos de la videotécnica ha de ser apropiada para la emisión del juicio de necesidad, cuya valoración será mucho más fácil si los mencionados fines se encuentran convenientemente descritos en un documento *ad hoc*[71].

La licitud de las videocámaras, según lo establecido en el § 6b BDSG, se hace depender de que la videovigilancia sea necesaria, es decir adecuada para lograr los objetivos fijados previamente y no exista otro medio igual de efectivo que pudiera limitar en menor medida el derecho a la audoterminación informativa de los afectados por ella. Por tanto el empleo de estos sistemas no será legítimo cuando puedan alcanzarse a través de otros instrumentos menos invasivos los mismos fines. La seguridad de un local en ocasiones se puede garantizar por otros medios sin tener que acudir a la grabación de imágenes, por ejemplo, reformándolo simplemente para mejorar su iluminación, o contratando a personal para que custodie sus accesos. En todos estos supuestos también el aspecto económico debe ser tomado en consideración

[70] Duhr, E.; Naujok, H.; Peter, M. y Seiffert, E., «Neues Datenschutzrecht für die Wirtschaft, Erlaüterungen und praktische Hinweise zu § 1 bis 11», *Datenssicherheit und Datenschutz*, 2002, p. 28. Duhr, E.; Naujok, H.; Peter, M.; Seiffert, E., «Neues Datenschutzrecht für die Wirtschaft, Erlaüterungen und praktische Hinweise zu § 27 bis 46», *Datenssicherheit und Datenschutz*, 2003, p. 7.

[71] «Begrundung zur Beschlussempfehlung des Innenauschusses», *BT-Drs*, 14/5793, p. 61.

porque a los propietarios de los inmuebles no se les puede exigir el desembolso de una ingente suma de dinero para garantizar su seguridad.

Resulta muy ilustrativo en este sentido la sentencia del Tribunal de Berlín centro, de 18 de abril de 2003, en la que el órgano juzgador se pronunció acerca de la licitud de un sistema de videovigilancia emplazado en los exteriores de un conocido centro de compras de la capital alemana, el *Kulturkaufhaus* Dussmann. En concreto el pronunciamiento se refiere a los sistemas de vigilancia situados en las arcadas de uno de los frentes del edificio, a los ubicados en la pared exterior y al colocado a un metro de distancia de la vía pública.

Las cámaras se colocan por el propietario del inmueble para la observación y registro de imágenes con la finalidad de tutelar la seguridad de los clientes, evitando posibles robos o atracos, así como también con el objetivo de proteger la integridad del edificio frente a grafitos, o daños en los escaparates por arañazos, rotura de cristales, etc. El demandante en este caso es un periodista que debido a su profesión frecuenta el centro de Berlín, y afirma que pasa al año por delante del centro comercial una media de 70 a 80 veces en horario diurno y de 5 a 6 veces en horario nocturno.

En la sentencia se planteó, primero, si el pasillo con arcos del *Kulturkaufhaus* Dussmann en el que se emplazaron las cámaras, es simplemente un lugar de paso o si por el contrario era utilizado de forma espontánea para la comunicación y conversación por parte de los viandantes. Si se trataba de esta segunda opción el nivel de protección que se le debía dispensar al lugar citado tendría el más alto por ser aquí en donde las personas conversaban o se relacionaban. El órgano judicial sin embargo entendió, primero que no se trataba de un sitio adecuado para permanecer durante largo tiempo por encontrarse en el medio de una vía de paso. Y asimismo, consideró, en segundo lugar, que el derecho a la autodeterminación informativa del recurrente no resultaba afectado por la presencia de estas cámaras. Según el Juzgador, el demandante en ningún momento afirmó realizar ese tramo del camino a pié y en todo caso aunque así fuera, sostuvo que no era posible a través de las imágenes obtenidas por la videocámara una identificación de las personas que regularmente por allí transitaban por la distancia que generalmente mantenían al pasar por delante de la fachada del edificio.

El Tribunal consideró la posibilidad de incorporar personal al centro comercial para que lo vigilase las 24 horas pero inmediatamente descartó esta solución debido a los elevados costes económicos que ello supondría habida cuenta de que la observación debía ser continuada y de que se trataba de un edificio de gran tamaño y complejidad. Asimismo, estimó el Juzgador que la videovigilancia establecida fundamentalmente en este caso para la persecución de los delitos y la reclamación de posibles daños difícilmente podía ser sustituida por la observación efectuada a través el ojo humano. Según el Tribunal de Berlín esta última no es tan efectiva como la vigilancia de una

cámara que en ningún caso se puede equivocar y dispone además de medios que le permiten la identificación de la autoría de los hechos[72].

Con carácter general, el juicio de necesidad de tener que recurrir a la videovigilancia ha de realizarse de acuerdo con las prescripciones generales que se contienen en la ley. De este modo, el diseño y la selección de los sistemas de tratamiento de datos se guiará por el principio de no recogida, tratamiento o utilización de los mismos o en caso hacerlo por el del menor número posible en el sentido expresado por el § 3a de la BDSG. Asimismo la observación mediante cámaras tendrá que limitarse tanto espacial como objetivamente. Esto implica que durante una continuada observación la función del *zoom* no debe permanecer activada constantemente sino ocasionalmente, es decir, deberá ponerse en funcionamiento a través de impulsos concretos como ocurre, por ejemplo, con los sistemas de videos que se incorporan a los porteros automáticos. Igualmente debe renunciarse a las genéricas y amplias grabaciones cuando existen otras alternativas que conducen a los mismos resultados, en concreto no son necesarios los sistemas que permiten que las imágenes puedan ser transmitidas a través de Internet o Intranet.

Estas exigencias deben ser especialmente respetadas cuando en el local de acceso público se encuentran también en puestos de trabajo, pues el empresario garantizará a los trabajadores a través del acondicionamiento del sistema que van a permanecer ciertos ámbitos situados fuera del control de observación de los aparatos de videovigilancia.

7. PONDERACIÓN DE LOS INTERESES EN JUEGO

La videovigilancia será lícita, de acuerdo con lo que establece el apartado primero del § 6b BDSG, si es necesaria, en primer lugar; y en segundo lugar, si no hay elementos que permitan suponer que existen intereses dignos de protección que deban prevalecer derivados del derecho a la autodeterminación informativa de las personas observadas.

Los derechos de los sujetos pasivos no se entenderán lesionados si, como consecuencia de la cualidad de la grabación, no es posible su identificación. Por ejemplo, las grabaciones que se efectúan en las plazas privadas del parking de una vivienda a través de un circuito cerrado de televisión no plantean ningún conflicto porque generalmente la resolución de las cámaras es de tan baja calidad que ni la identificación de las personas ni tampoco las de las matrículas de los vehículos es posible[73].

[72] *Bundesdatenschutzgesetz Dokumentation*. 38 Lieferung der Gesamtdokumentation, Juli, 2005, pp. 1-8. *Datenschutz und Datensicherheit*, 2004, págs 309-312. *Neue Juristische Wochenschrift-Rechtsprechungs-Report Zivilrech*t 2004, pp. 531-534.

[73] WEDDE, P., «Videoüberwachung. § 6b»*, op. cit.,* p. 244.

En la actualidad, sin embargo, los problemas derivados de la reproducción de vídeos se multiplican porque los modernos sistemas de videovigilancia poseen una resolución cada vez mayor, lo que representa una amenaza constante para los derechos de la personalidad.

De acuerdo con el § 3 I BDSG, los afectados por estos procedimientos no son solo las personas fácilmente identificables sino también todas aquéllas que pueden serlo a través de una información adicional. Las razones para proteger sus derechos tienen que existir realmente y basarse en hechos comprobables aunque no se requiere su prueba. Las sospechas especulativas no son sin embargo suficientes.

La tutela de los intereses de los afectados prevalece cuando el objetivo de las cámaras es la vigilancia de una persona aislada o en los supuestos en que los afectados no pueden apartarse del lugar objeto de la observación. Son ilegales, por ejemplo, las cámaras en los vestuarios o en los aseos aunque sea con la finalidad de prevenir robos, hurtos u otros actos violentos.

Por regla general la injerencia en los derechos de la personalidad a través de la observación no es tan intensa como en los casos de registro o transmisión de imágenes. De igual manera que la continua y permanente vigilancia de un lugar que los afectados no pueden abandonar supone un atentado más grave para los derechos de la personalidad que si es temporal y está circunscrita a concretos espacios del lugar observado. Por ejemplo puede suceder que todos los coches, trenes y vagones de metro de una empresa de transporte estén equipados con videocámaras y no exista posibilidad alguna de sortearlas porque en la mayoría de los casos el transporte de personas de cercanías e incluso el de largos trayectos se encuentra en régimen de monopolio. Los pasajeros dependen regularmente de su utilización y no tienen la posibilidad de acudir a otros medios de locomoción. En estas situaciones, según la opinión de algunas autoridades de vigilancia y una parte de la doctrina jurídica, existen suficientes motivos para entender que los intereses de los afectados deben prevalecer sobre todo si en estos transportes no existen zonas fuera de la mirada de las cámaras, por ejemplo, en alguno de los vagones del metro, del tren o en una parte del autobús[74].

La permanente vigilancia en una entrada o salida de un edificio o de un local es legalmente permisible, si aún cuando existe iluminación y controles, siguen produciéndose daños y desperfectos. Con carácter general es necesario realizar una ponderación de los intereses en juego objeto de protección constitucional que pudieran resultar afectados por la observación en cada caso concreto examinando todas y cada una de las circunstancias y de los derechos en juego. El registro de las imágenes solo podrá llevarse a cabo de manera excepcional según el Tribunal Supremo alemán cuando se producen agresiones graves a los derechos de los responsables, algo así como ataques

[74] LANG, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), p. 301.

a su persona o al ámbito directo de la vivienda que no podían ser reparados de otra forma. Un supuesto típico en este contexto se plantea cuando determinados espacios o establecimientos están especialmente amenazados, por ejemplo, la entrada de un edificio en la que se ha cometido más de un acto violento. En estos casos pasarán a un segundo plano los intereses de los afectados, al contrario de lo que sucede con las imágenes que pudieran ser obtenidas en los aseos o en las consultas de un médico en donde en ningún caso ocurre esto[75].

La necesidad de ser protegido frente a las cámaras en los lugares públicos varía dependiendo del lugar de que se trate. La literatura jurídica diferencia entre ámbitos en los cuales el desarrollo de la personalidad o la garantía de los derechos de la libertad tienen una gran relevancia de otros en que posee mucha menor importancia. Dentro del primer grupo se encuentran, por ejemplo, las salas de espera de los medios de transporte, los restaurantes, los parques de atracciones o los lugares de entretenimiento, en los que las personas se comunican, comen, beben o simplemente se relajan. Los observados por la videovigilancia en estos lugares deben ser objeto de mayor protección que los que se encuentran en otros espacios en los cuales el desarrollo de la personalidad o la garantía de los derechos no es tan típica, como sucede, por ejemplo, en los lugares de tránsito, en las antesalas de los bancos, en las gasolineras o en los mostradores de los locales comerciales[76].

En este sentido resulta muy ejemplificativo el siguiente caso que ha sido resuelto por el Tribunal de trabajo de Hamburgo en la sentencia de 22 de abril de 2008[77]. El asunto es el siguiente: el dueño de una cadena de cafeterías la citada ciudad alemana decidió instalar en sus locales sistemas de videovigilancia. Las cámaras se repartían por todas las salas en las que se ubicaban los mostradores y las estanterías con mercancías en las cuales los clientes solicitaban sus consumiciones y efectuaban sus pagos, también se instalaron cámaras en los lugares de reunión, es decir en donde los clientes se sentaban a charlar y a disfrutar de sus consumiciones. El demandante del caso, cliente habitual de estos locales, entendió que se vulneraba su derecho a la autodeterminación informativa reconocido en el artículo 2 de la Constitución alemana por la presencia constante de videocámaras en los espacios equipados con mesas y solicitó su retirada.

El demandado que disfrutaba indiscutiblemente del derecho de morada en todas sus cafeterías, invocó para su defensa en este caso particular la doble finalidad de la videovigilancia. Por un lado, preventiva, para evitar la comisión de robos y sustracciones que se pudieran cometer por parte de los clien-

[75] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), p. 301.

[76] Lang, M., *Private Videoüberwachung im öffentlichen Raum, op. cit.* (nota 41), p. 305.

[77] *Bundesdatenschutzgesetz Dokumentation*. 47 Lieferung der Gesamtdokumentation. Juni 2009, pp. 1-5.

tes en sus locales; y, por otro, represiva, con el objetivo de asegurar las pruebas que pudieran ser de utilidad en aras a la persecución de los delitos. La videovigilancia, según manifestó el Tribunal, era el instrumento adecuado para alcanzar los objetivos regulados en el § 6b I BDSG. A su juicio no existía ningún otro medio menos invasivo con el que el demandado pudiera tutelar sus intereses. La contratación de personal de seguridad se descartaba por el elevado gasto que ello podría suponer. Por lo que se refería a la persecución del delito, según entendió el Juzgador, resultaba evidente que la declaración de un vigilante como testigo ocular no era tan efectiva como la grabación de una cámara. Mientras que el ojo humano se podía equivocar en alguna ocasión la videocámara no cometía este tipo de errores.

Los intereses que se encontraban en juego en este conflicto eran, por una parte, los derivados del derecho fundamental a la autodeterminación informativa reconocido el artículo 2.1º de la Constitución germana, y por otra, los del demandado, que eran los derechos fundamentales al desarrollo libre de la profesión y el derecho de propiedad de la empresa previstos en los artículos 12 y 14, respectivamente, del mismo Texto legal.

El Tribunal consideró que era necesario diferenciar en este supuesto entre los lugares en los que se encontraban los mostradores y las estanterías con las mercancías de aquellos otros en los que tranquilamente se reunían los clientes para charlar y disfrutar de sus consumiciones. En los segundos, el derecho a la autodeterminación informativa invocado por el reclamante garantizaba que cada uno pudiera moverse públicamente de manera libre sin el temor de ser objeto de videovigilancia, debiendo prevalecer en estos lugares teniendo en cuenta las circunstancias y las características de los mismos los intereses del reclamante. En líneas generales, a jucio del Tribunal, la necesidad de protección en los lugares en donde existe un mayor riesgo de que se produzcan robos o cualquier tipo de sustracción es más alto que en aquellos espacios en donde se ubican las mercancías y los mostradores de atención al público. Es aquí en donde se justificaba y admite la inclusión de sistemas de videovigilancia mientras que en los lugares de reunión en donde los clientes conversan y disfrutan de sus consumiciones no existe ningún peligro y por tanto no tiene sentido la colocación de estos sistemas. Para finalizar el Juzgador añadió, que por ser habitáculos en donde los clientes permanecen una gran parte observados de forma continua pueden verse amenazados gravemente sus derechos de la personalidad.

8. OBLIGACIÓN DE SEÑALIZACIÓN

El § 6b II BDSG prevé que tanto la instalación de videocámaras como del órgano responsable de las mismas en un determinado lugar deberán darse a conocer a través de medidas idóneas. Su existencia se hará notar o bien a través de señales en varios idiomas –en caso de probable presencia de ciudadanos

extranjeros, como sucede, por ejemplo, en los aeropuertos o en las estaciones de tren– o bien, mediante pictogramas que suelen ser claros y de fácil comprensión. Es a estos últimos a los que se recurre en la generalidad de las ocasiones.

El organismo encargado de las videocámaras al que asimismo le corresponderá garantizar los derechos de los afectados aparecerá claramente indicado, figurando el nombre y la dirección completa no siendo suficiente únicamente con el apartado postal. Un modo podría ser: «Este edificio es videovigilado por la empresa x. Si tienen alguna pregunta dirijanse por favor a …». El mismo objetivo de transparencia perseguido por la ley se logra también en aquellos casos en los que aunque no existen señales anunciadoras de la videovigilancia figura cuál es el organismo responsable[78].

El Tribunal laboral de Frankfurt en una sentencia de 25 de enero de 2006 rechazó la aportación al proceso de unas imágenes captadas por unas videocámaras. El empresario, dueño de un local de venta de bebidas, había instalado el sistema de videovigilancia sin ponerlo en conocimiento de sus trabajadores. El Juzgador consideró que trataba de una medida ilícita y, en consecuencia, no valoró el material obtenido por las cámaras[79].

Ahora bien, es cierto también que en ocasiones se prevén excepciones a esta obligación de señalización de la videotécnica prevista en la Ley federal de Protección de datos. El Tribunal del *Land* de Berlín en una sentencia de 18 de noviembre de 2010 consideró que en este supuesto la instalación de videovigilancia de manera secreta era conforme con la Constitución. El empresario se encontraba en una situación que fue definida como de legítima defensa. Tenía sospechas fundadas de que sus trabajadores habían cometido algunos delitos en horario laboral, y el empleo de otros instrumentos de investigación menos agresivos con los derechos de sus empleados para averiguar lo sucedido no había tenido éxito. La videovigilancia era el único medio disponible a su alcance para resolver sus dudas. El Juzgador, a la vista de las circunstancias del caso, entendió que se trataba de una medida lícita aún cuando la presencia de cámaras no estaba señalizada[80].

9. OBLIGACIÓN DE COMUNICACIÓN

Según establece el § 6b IV BDSG, cuando los datos recogidos mediante videovigilancia se adscriban a una persona determinada, ésta habrá de ser

[78] Gola, P. Y Schomerus, R., «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen», *op. cit.,* Rn 27. En J:\Gola-Schomerus, BDSG § 6b Rn_24 - 28a - beck-online.mht.

[79] *Bundesdatenschutzgesetz. Dokumentation.* 43 Lieferung Gesamtdokumentation. November, 2007, págs 1-6.

[80] *Bundesdatenschutzgesetz Dokumentation*. 51 Lieferung der Gesamtdokumentation. April, 2011, pp. 1-4.

informada sobre el tratamiento o la utilización de los mismos. Los preceptos en los que se regula esta cuestión son el § 19a y el § 33 de la norma citada. El primero contempla el tratamiento de datos por parte de las entidades públicas, y el segundo –que es el que aquí nos interesa– regula esta materia cuando los órganos responsables son las empresas y las entidades no públicas.

El § 33 BDSG dispone que cuando se registren por primera vez datos personales para fines propios sin el conocimiento del interesado, habrá de comunicársele a éste el registro, el tipo de datos, la finalidad de la recogida, el tratamiento o utilización de los mismos y la identidad de la entidad responsable. Si se registrasen comercialmente a efectos de transmisión desconociéndolo el interesado será informado de la primera transmisión y también de qué clase de datos se trata.

En el mismo precepto se recogen una serie de supuestos en los que la comunicación al interesado no será obligatoria: si éste tiene noticia del registro o de la transmisión por otra vía; cuando los datos no pueden cancelarse o están destinados exclusivamente a garantizar la seguridad o el control de su protección y una comunicación requiriese un despliegue de medios extraordinario; en los supuestos en que los datos deben mantenerse en secreto en virtud de una disposición legal o por su naturaleza el registro o la transmisión de los mismos están expresamente previstos por ley; en los casos en los que el registro o la transmisión son necesarios para fines de investigación científica y la comunicación exigiera un despliegue de medios desproporcionado; en aquellas situaciones en que la entidad pública competente ha constatado frente a la entidad responsable que la publicación de los datos pudiera poner en peligro la seguridad o el orden públicos o perjudicar de otro modo el bien de la Federación o de un Estado federado; y por último, cuando los datos están registrados para fines propios y comercialmente resulta desproporcionada su transmisión y comunicación por la gran cantidad de casos afectados.

10. TRATAMIENTO Y UTILIZACIÓN DE LOS DATOS

La recogida, el tratamiento y la utilización de datos personales solo serán lícitos cuando se autorice o disponga legalmente o bien en los casos en los que el interesado haya manifestado su consentimiento. Los audiodatos no se incluyen dentro de este régimen porque, evidentemente, no se puede acceder a ellos a través de la observación sino a través de otros aparatos que no aparecen previstos en el precepto en cuestión[81].

La necesidad de acudir a estas técnicas deberá juzgarse teniendo en cuenta los mismos criterios que en el caso de la observación, es decir, habrá de valorarse si la recogida, el tratamiento o la utilización de los datos personales

[81] LANG, M., *Private Videoüberwachung im öffentlichen Raum*, *op. cit.* (nota 41), p. 321.

son imprescindibles para alcanzar los fines previstos y si no existen otros medios más apropiados y menos restrictivos con el derecho a la autodeterminación informativa de los afectados. No es necesario para poder acudir al tratamiento y utilización de los datos que sean indispensables para la consecución del objetivo perseguido pero sí que habrá que plantearse llegado el caso si basta con otros procedimientos menos invasivos, como por ejemplo la observación para lograr los mismos fines[82].

De acuerdo con lo dispuesto por el precepto estas actividades de tratamiento y utilización de datos son conformes a derecho, primero, si son necesarias para la finalidad prevista que deberá establecerse inicialmente desde el mismo momento en que se acuerda la instalación de la videovigilancia. En caso de producirse una modificación posterior de la adscripción prevista ésta será considerada ilegal. En segundo lugar, es preciso tener en cuenta que no existan otros elementos que permitan suponer que hay intereses dignos de protección del interesado preponderantes. Su presencia no es necesario que sea demostrada pero tampoco basta con la simple incertidumbre acerca de su posible existencia[83]. En casos de duda o sospecha deberá decidirse a favor del afectado para dejar a salvo su derecho a la autonomía personal.

Las tareas de tratamiento y utilización de los datos personales son posibles si se cuenta con autorización del interesado. Únicamente su intervención no será necesaria, primero, si así lo prevé o permite una disposición legal; segundo, si la tarea administrativa específica o la finalidad comercial requiere una recogida de datos recurriendo a otras personas o entidades; y tercero, si el tener que recurrir al afectado supusiera un despliegue de medios desproporcionado y no existiesen otros elementos que permitan suponer que se están perjudicando intereses diversos que deban ser tomados en consideración[84].

Los datos obtenidos a través de la observación únicamente podrán tratarse o utilizarse por regla general con la finalidad originaria con la que la videovigilancia fue instalada. La ruptura de estos objetivos únicamente será posible en tanto sea necesario, por un lado, para evitar peligros para la seguridad estatal y pública y por otro, para la persecución de los delitos. Por ejemplo, las imágenes de vídeo obtenidas en un centro comercial solo serán enviadas y posteriorme examinadas si tras haberse cometido un delito se pudieran encontrar en ellas algún tipo de indicio acerca del posible autor[85].

La valoración de la necesidad se realiza teniendo en cuenta los mismos principios que se aplican para la observación. Es decir, habrá que examinar si el registro, comunicación, tratamiento o utilización de los datos personales

[82] Lang, M., *Private Videoüberwachung im öffentlichen Raum*, *op. cit.* (nota 41), p. 322.
[83] Wedde, P., «Videoüberwachung. § 6b», *op. cit.* (nota 35), p. 246.
[84] § 6b III BDSG.
[85] Wedde, P., «Videoüberwachung. § 6b», *op. cit.* (nota 35), p. 247.

para las finalidades previstas es necesario y si no existen otros intereses que deban ser objeto de una protección mayor. Por ejemplo, en los taxis, autobuses, trenes y metros, una observación directa de todos los pasajeros no es posible. Por eso los datos han de ser almacenados al igual que sucede también en otros ámbitos como por ejemplo, gasolineras o cajeros automáticos de bancos en donde es necesario el empleo de estas técnicas.

11. CONTROL PREVIO

Si los procesos de tratamiento automatizado de datos revisten riesgos especiales para los derechos y libertades de los interesados serán objeto de un control previo[86]y el encargado de efectuarlo es el delegado para la protección de datos. Nos estamos refiriendo aquí, por ejemplo, a camáras de videovigilancia que son orientables y disponen de una alta resolución para la captación de las imágenes, o a *webcams* que efectúan descargas en Internet. Únicamente no se efectuará este control previo si existe una obligación legal; si media consentimiento del interesado; o en último lugar, en aquellas ocasiones en las que la recogida, tratamiento o utilización de las imágenes se efectúan para fines contractuales o cuasicontractuales con el interesado[87].

12. OBLIGACIÓN DE CANCELACIÓN DE LOS DATOS

Según la BDSG los datos se cancelarán tan pronto como dejen de ser necesarios para la finalidad prevista o existan intereses dignos de protección contrarios a su conservación.

En el ámbito de la videovigilancia cuando se habla de «datos» se está refiriendo a datos personales almacenados. Esto se deduce de la sistemática y del concepto legal de suprimir contenido en la BDSG en donde se define esta acción como la cancelación de los datos personales registrados (§ 3 IV n° 5 BDSG). Esta operación debería estar protegida través de una técnica automática y de un sistema manual que únicamente fuera posible activar en una situación de peligro sobrevenida. Nos referimos a datos que han sido clasificados, incluidos o conservados sobre un soporte al objeto de tratarlos o utilizarlos nuevamente[88].

De acuerdo con el tenor literal del § 6b V BDSG, los datos serán cancelados. Primero, cuando dejan de ser necesarios para la finalidad prevista tanto

[86] § 4d V BDSG.

[87] Gola, P. Y Schomerus, R., «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen», *op. cit.*, Rn 9. En J:\Gola-Schomerus, BDSG § 6b Rn_ 8 - 9 - beck-online.mht.

[88] Bizer, J., «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen», *op. cit.* (nota 33), pp. 602-603.

si ésta se ha cumplido o no y ya no son necesarios. Segundo, si existen intereses dignos de protección contrarios a la conservación de la grabación misma. En el primer caso puede o no haberse producido el almacenamiento de los datos mientras que en el segundo supuesto esta operación siempre se ha producido y es preciso proceder a la supresión de los mismos de modo inmediato aun cuando pudieran ser útiles para alcanzar otros objetivos[89]. La doctrina entiende que para su cancelación no es preciso que concurrran las dos circunstancias sino que basta con una de ellas. Puede ocurrir que atendiendo al primer presupuesto sea necesario conservar los datos y por el contrario haya que proceder a eliminarlos en aplicación de la segunda condición. Sería posible, por ejemplo, que en un procedimiento de investigación y persecución de un ilícito no se desarrollase ágilmente dentro de los plazos razonables y de esa forma la cancelación de demorase de manera desproporcionada[90].

El precepto no establece con carácter general un tiempo concreto para la eliminación de los datos. Deberá fijarse teniendo en cuenta, por un lado, la finalidad perseguida con la grabación y por otro, la proporcionalidad, a la vista de los intereses de los afectados. En consecuencia, la licitud de la duración es muy diferente dependiendo de las circunstancias de cada caso concreto.

Cuando se instala videovigilancia en los taxis para evitar robos, se entiende que 24 horas son suficientes para el almacenamiento de las imágenes; en tranvías y buses, la media se sitúa entre 24 y 48 horas respectivamente; tiempos que puede variar dependiendo del *Land* de que se trate; y en el caso del metro la media gira en torno a las 24 horas. En los centros comerciales se considera que 2 días como mínimo son necesarios aunque es cierto también que el tamaño del negocio es un factor a considerar porque en las grandes superficies es más difícil detectar si se han producido daños o se ha cometido alguna sustracción. En el caso de los cajeros automáticos puede ser necesario un almacenamiento de los datos durante semanas o incluso, en algunos casos, durante meses, para que la videovigilancia pueda cumplir con la finalidad prevista[91].

13. DERECHO DE LOS LÄNDER

Los *Länder* de Baviera (§ 21a), Berlín (§ 31b), Brandenburgo (§ 33c), Bremen (§ 20b), Mecklemburgo-Pomerania Occidental (§ 37), Renania del Norte-Westfalia (§ 29b), Renania-Palatinado (§ 34), Sarre (§ 34), Sajonia (§ 33), Sajonia-Anhalt (§ 30) y Schleswig-Holstein (§ 20) han incluido en sus leyes de protección de datos una norma relativa a la videovigilancia cuyo

[89] WEDDE, P., «Videoüberwachung. § 6b», *op. cit*. (nota 35), p. 248.

[90] «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen», *op. cit*., p. 603.

[91] LANG, M., *Private Videoüberwachung im öffentlichen Raum*, *op. cit.* (nota 41), p. 330.

contenido coincide básicamente con el previsto en § 6b de la BDSG a nivel federal[92]. Las diferencias de regulación existentes entre el nivel federal y estatal son mínimas. En Berlín, por ejemplo, la Ley ha establecido excepciones a la obligación de comunicación de los datos personales (§ 31 b 4 3). El § 29b II DSG[93] de Renania del Norte-Westfalia dispone que los datos grabados a través de videovigilancia únicamente pueden ser almacenados en caso de que exista algún peligro. Por lo que se refiere a la obligación de cancelación, en Bremen los datos grabados son borrados, como más tarde, en 24 horas (§ 20b V), en Renania Palatinado serán eliminados de inmediato (§ 34 V) mientras que Mecklemburgo-Pomerania Occidental (§ 37 II) y Schleswig-Holstein (§ 20 II) tienen un plazo más amplio para su supresión: siete días[94].

14. CONCLUSIONES

La aplicación de los sistemas de videovigilancia para garantizar la seguridad ha contribuido a la prevención y persecución del delito, pero, al mismo tiempo, ha sido una fuente generadora de problemas, en la medida en que ha supuesto, en muchos casos, un sacrificio excesivo de derechos y libertades como el derecho a la intimidad o a la protección de datos.

La legislación alemana se ha preocupado de regular con gran detalle la videovigilancia pública, es decir, la efectuada por las Fuerzas y Cuerpos de Seguridad, ámbito en el que existen numerosas disposiciones legales y pronunciamientos jurisprudenciales, tanto del Tribunal Constitucional como de los jueces y tribunales ordinarios, así como abundantes estudios doctrinales que se han ocupado con profusión del tema. Por el contrario, en el caso de la videovigilancia privada en espacios de acceso público, a pesar de su enorme expansión en los últimos años, la normativa es escasa y sorprende igualmente la poca atención que le ha prestado la literatura especializada.

La regulación legal de la videovigilancia privada en los lugares de acceso público se aborda fundamentalmente, en el derecho alemán, desde la perspectiva del derecho a la autodeterminación informativa. Tanto en el ámbito federal como en el estatal las leyes de protección de datos contienen un precepto específico dedicado a su previsión normativa. En el § 6b BDSG se recogen los principios generales del derecho a la protección de datos en materia

[92] En los parágrafos que aparecen vinculados a los distintos Länder es en donde se contiene la regulación sobre videovigilancia en las Leyes de Protección de datos de estos Estados alemanes.

[93] *Datenschutzgesetz* o Ley de Protección de Datos de 9 de mayo de 2000 de Renania del Norte-Westfalia (Gesetz und Veordnungsblatt, p. 452).

[94] GOLA, P. y SCHOMERUS, R., «§ 6b Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen», *op. cit.*, Rn 34. En J:\Gola-Schomerus, BDSG § 6b Rn_ 34 - beck-online.mht.

de videovigilancia: su definición, los supuestos en que se entiende conforme a derecho, la obligación de señalización y los principios que se han de seguir en los casos de tratamiento y utilización de los datos personales obtenidos. Todavía existen, sin embargo, importantes cuestiones que no han quedado resueltas en el ámbito legal, lo que provoca dudas sobre el régimen jurídico aplicable. Así, el § 6b BDSG regula la videovigilancia en lugares de acceso público, pero no define cuáles son, qué características tienen que reunir ni qué ocurre con aquellas estancias que poseen una naturaleza mixta, esto es, que se encuentran a caballo entre el carácter privado y el público. Tampoco se precisa qué otros aparatos tecnológicos (además de las videocámaras) deben ser catalogados como equipamientos óptico-electrónicos, ni si tienen el mismo tratamiento legal que aquéllas.

Tras analizar los supuestos en que según el § 6b BDSG es lícita la videovigilancia en los lugares de acceso público se han descrito los principales problemas que se plantean con su aplicación práctica. En primer lugar, son difíciles de precisar los límites del *Hausrecht o* facultades de policía que les corresponden a los propietarios de los locales o a los responsables de los mismos. Es dudoso, por ejemplo, si se pueden grabar objetos o espacios que se encuentran colindantes a un camino público o a personas que circulan por él. En segundo lugar y por lo que se refiere al supuesto de la salvaguarda de intereses legítimos de fines específicamente previstos, existe una laguna legal en la regulación de las circunstancias y las competencias para la verificación de los objetivos.

Con carácter general, la licitud de las videocámaras se hace depender tanto de que la videovigilancia sea necesaria, es decir adecuada para lograr los objetivos fijados previamente, como de que no exista otro medio igual de efectivo que pudiera limitar en menor medida el derecho a la audoterminación informativa de los afectados por ella.

Los jueces y tribunales ordinarios tienen un importante papel porque son los encargados de efectuar, si se produce algún conflicto, un juicio de ponderación en cada caso concreto, valorando si deben prevalecer los derechos de los afectados o el derecho del titular del local o espacio de acceso público a instalar estos instrumentos audiovisuales. En dicho juicio se toman diversos criterios en consideración, como son, por ejemplo, la temporalidad o el carácter permanente de la observación, si las cámaras son fijas o móviles, la calidad de resolución de las imágenes captadas por ellas, la zona concreta de ubicación de las mismas, los espacios prohibidos a la videovigilancia, etc.

Los Tribunales han excepcionado la obligación de señalización de los aparatos de grabación de la imagen en los casos en que existen sospechas por parte del empresario acerca de conductas ilícitas procedentes de sus empleados y no existen otros instrumentos de investigación menos agresivos con los derechos de los trabajadores para averiguar lo sucedido. En todo caso cuando las imágenes recogidas mediante videovigilancia se adscriban a una persona

determinada, ésta habrá de ser informada sobre el tratamiento o la utilización de las mismas.

El § 6b BDSG tambien establece la necesidad de que se proceda a una valoración de si la recogida, el tratamiento o la utilización de los datos personales son imprescindibles para alcanzar los fines previstos y no existen otros instrumentos más apropiados y menos restrictivos con el derecho a la autodeterminación informativa de los afectados. Las tareas de procesamiento de datos son posibles sin consentimiento del afectado, primero, si así lo prevé o permite una disposición legal; segundo, si la tarea administrativa específica o la finalidad comercial requiere una recogida de datos acudiendo a otras personas o entidades; y tercero, si el tener que acudir al afectado supusiera un despliegue de medios desproporcionado y no existiesen otros elementos que permitan suponer que se están perjudicando intereses diversos que deban ser tomados en consideración.

Por último, los datos obtenidos a través de la observación por videovigilancia únicamente podrán tratarse o utilizarse con la finalidad originaria con la que la que aquella fue instalada. La ruptura de estos objetivos únicamente será posible en tanto sea necesario, por un lado, para evitar peligros para la seguridad estatal y pública y por otro, para la persecución de los delitos. El precepto no establece con carácter general un tiempo determinado para la supresión de los datos sino que deberá fijarse teniendo en cuenta, de una parte, la finalidad perseguida con la grabación y la proporcionalidad, a la vista de los intereses de los afectados. Su cancelación se producirá, primero, cuando dejen de ser necesarios para los objetivos tanto si éstos se han cumplido o no. Segundo, si existen intereses dignos de protección contrarios a la conservación de la grabación misma. La doctrina entiende que para que se supriman las imágenes no es preciso que concurrran los dos requisitos sino que basta con uno de ellos, puede suceder que atendiendo al primer presupuesto sea necesario conservar los datos y por el contrario haya que proceder a eliminarlos en aplicación de la segunda condición o al revés. Sería posible, por ejemplo, que un procedimiento de investigación y persecución de un ilícito no se desarrollase ágilmente dentro de los plazos razonables y de esa forma la cancelación de demorase de manera desproporcionada. En consecuencia, el período de almacenamiento de las imágenes grabadas es muy diverso dependiendo de las circunstancias del supuesto concreto.

TITTLE: Private video surveillance in places of public access and data protection right. The German case.

SUMMARY: This work tries to offer an analysis of the regulation of privacy video surveillance in places of public access in the German Law from the point of view of data protection right. The central core of this study is the examination of the paragraph 6b of the federal Law of data protection

and of the jurisprudence dictated on this question in which does not forget the most important doctrinal reflections on the topic either.

Key words: Freedom, Security, Video Surveillance, Fundammental rigths, Data protection right, Privacy right.

Resumen: Este trabajo tiene por objeto el examen de la regulación de la videovigilancia privada en los lugares de acceso público en el derecho alemán desde la perspectiva del derecho a la protección de datos. El análisis del parágrafo 6b de la Ley federal de protección de datos y de la jurisprudencia dictada sobre esta materia constituyen el núcleo central de este estudio en el que tampoco se olvidan las reflexiones doctrinales más importantes sobre el tema.

Palabras clave: Libertad, seguridad, videovigilancia, derechos fundamentales, derecho a la protección de datos, derecho a la intimidad.

Recibido: 21.03.2014
Aceptado: 26.05.2014