Facultad de Ciencias Sociales y Jurídicas

Grado en Derecho

Trabajo Fin de Grado

UNA APROXIMACIÓN A LOS LÍMITES DE LA VIDEOVIGILANCIA

Alumno: Carlos Serna Perales

Enero, 2020

Universidad de Jaén
Facultad de Ciencias Sociales y Jurídicas

RESUMEN/ABSTRACT DEL TRABAJO FIN DE GRADO

TÍTULO DEL TRABAJO DE FIN DE GRADO	UNA APROXIMACIÓN A LOS LÍMITES DE LA VIDEOVIGILANCIA
AUTOR	CARLOS SERNA PERALES
GRADO	DERECHO Y DIR. Y ADMÓN. DE EMPRESAS
TUTOR	MARÍA JOSÉ CARAZO LIÉBANA
DEPARTAMENTO	DERECHO CONSTITUCIONAL
Resumen en castellano	En este trabajo, podrá encontrar algunas limitaciones que regulan el uso de las cámaras de seguridad y que impiden dañar el derecho a la intimidad y a la protección de datos de las personas que son grabadas por estos instrumentos. Para ello analizaremos distintos ámbitos en los que la videovigilancia se encuentra limitada, facilitando así el uso de este tipo de sistemas al usuario. En este documento, el lector podrá verse identificado con una serie de casos que han tenido una relevancia importante tanto en los tribunales españoles como en nuestra sociedad y que son tratados desde el punto de vista de la protección de datos.
Resumen en inglés	In this work, you can find some restrictions which regulate the use of the security cams and avoid damaging the right to privacy and the right to data protection of the people who are recorded by these instruments. That is why we are analyzing different scopes where the video surveillance is limitated, making easier the use of these systems to the user. In this document, the reader can be identified with some cases which have had a great relevance both in Spanish courts as in our society and which are treated from the data protection's point of view.

Código UNESCO	Descriptor castellano	Descriptor inglés
5605.04	Derecho constitucional	Constitutional law

Nomenclatura Internacional de UNESCO para Ciencia y Tecnología:
http://skos.um.es/unesco6/

Jaén, 20 de enero de 2020

Fdo.: Carlos Serna Perales

Universidad de Jaén
Facultad de Ciencias Sociales
y Jurídicas

A/A SRA. PRESIDENTE DE LA COMISIÓN DE TRABAJO FIN DE GRADO DE LA FACULTAD CIENCIAS SOCIALES Y JURÍDICAS DE LA UNIVERSIDAD DE JAÉN

Índice

1. INTRODUCCIÓN

Hemos elegido este interesante y amplio ámbito de la protección de datos por su importancia en la protección de las personas y de sus datos personales, pues, a la vez que constituye una medida de protección, supone una gran limitación a la intimidad de las personas.

El dato personal que se tratará a través de la videovigilancia es la imagen, dato en el que profundizaremos más adelante y que constituye un dato muy importante para las personas.

En este sector de la protección de datos podemos encontrar múltiples dilemas acerca de su funcionamiento y finalidad, pues cuenta con una serie de limitaciones que trataremos con el fin de facilitar el uso de videocámaras de seguridad y su avance en el tiempo mediante las nuevas tecnologías.

Por otro lado, aunque cualquier persona puede, a día de hoy, instalar un sistema de videovigilancia o utilizar este tipo de cámaras, pocos conocen las indicaciones y limitaciones que impone la legislación y la jurisprudencia, de tal forma que los derechos de las personas y sus datos personales pueden verse afectados por esos usos inapropiados de la videovigilancia.

Es por esto que, a lo largo de este trabajo, encontraremos algunos de los límites a los que se encuentra sometido el control por cámaras de seguridad, observados desde distintos aspectos, de tal forma que el lector pueda conseguir una visión global sobre el ámbito de la videovigilancia.

Iniciaremos nuestro recorrido por los límites del control mediante videocámaras analizando la imagen como tal y el derecho atribuido a las personas a proteger su intimidad.

Seguiremos con una diferenciación entre el tratamiento de la imagen y de la voz, hechos estos que suponen algunas dificultades para las personas de a pie que pretenden hacer uso de estas herramientas de captación de datos.

A continuación, se hará hincapié en la importancia y valor que tiene la señalización de una zona videovigilada en la protección de datos, analizando algunos de los casos que pueden ser conflictivos en este ámbito.

Junto a esto, se hará una breve mención a la limitación temporal que existe para el tratamiento de datos personales obtenidos a través de un sistema de cámaras de seguridad.

Una vez analizadas las bases y limitaciones básicas, pasaremos a tratar una serie de casos que han asentado jurisprudencia en nuestro país en el ámbito laboral, en los que

existe un grave conflicto entre la intimidad de los interesados/afectados y la facultad que se le otorga al empleador para ejercer un control sobre la actividad de sus empleados.

A ello uniremos un conjunto de circunstancias cotidianas en las que podemos encontrar sistemas de videovigilancias y para las que existe un procedimiento previo de aprobación concreto para la instalación de éstas.

Para finalizar este trabajo, analizaremos el papel que tienen los Cuerpos y Fuerzas de Seguridad del Estado en la videovigilancia de los espacios públicos y cómo están incorporándose las nuevas tecnologías a la videovigilancia, llevando consigo la elaboración de una nueva normativa que regule su uso.

2. LA IMAGEN Y EL DERECHO A LA INTIMIDAD COMO PILARES DEL TRATAMIENTO.

Tal y como mencionamos en la introducción, la videovigilancia tiene como fin el tratamiento de la imagen. Esta imagen se encuentra ligada a la intimidad personal y familiar de las personas.

La Constitución decidió reunir en un mismo precepto, el apartado 1 del artículo 18, el derecho a la intimidad personal y familiar y a la propia imagen, los cuales se regulan y desarrollan en la Ley Orgánica 1/1982[1], de 5 de mayo, *de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*. Sin embargo, a continuación, trataremos ambos de forma separada, diferenciando entre la imagen como dato personal y el derecho a la imagen y a la intimidad.

Por su parte, tanto la Carta de los Derechos Fundamentales de la Unión Europea[2] como el Convenio Europeo de Derechos Humanos[3] hacen referencia a ese derecho a la vida privada de las personas.

2.1. La imagen

Aunque parece ser un concepto fácil y sencillo, no encontramos una definición de ésta en la legislación vigente. Así pues, para tener una aproximación a este elemento tan importante en nuestro trabajo, hemos de hacer uso de una de las instituciones más nobles

[1] Ley Orgánica 1/1982, de 5 de mayo, de protección civil de derecho al honor, a la intimidad personal y familiar y a la propia imagen. (enlace al documento: https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196)

[2] Carta de los Derechos Fundamentales de la Unión Europea, aprobada en Niza el 7 de diciembre de 2000. (enlace al documento: https://www.europarl.europa.eu/charter/pdf/text_es.pdf)

[3] Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, ratificado por España a 26 de septiembre de 1979 (enlace al documento: https://www.boe.es/buscar/doc.php?id=BOE-A-1979-24010)

y representativas de nuestra lengua, la Real Academia Española, que recoge en su amplio diccionario el concepto de imagen[4] desde un punto de vista óptico, el cual es el siguiente:

"Reproducción de la figura de un objeto por la combinación de los rayos de luz que proceden de él".

Junto a este concepto, el Diccionario de la Real Academia Española incorpora un subconcepto para la imagen virtual, que es el *"conjunto de los puntos aparentes de convergencia de los rayos luminosos que proceden de un objeto después de pasar por un espejo o un sistema óptico, y que, por tanto, no puede proyectarse en una pantalla"*.

En nuestra opinión, la imagen puede ser definida, a efectos del tema que aquí se trata, como esa captación de la realidad obtenida en un momento concreto del tiempo a través de un instrumento o sistema óptico y que puede ser contemplada o analizada con posterioridad. A estos efectos, debe entenderse por instrumento o sistema óptico cualquier objeto destinado a la captación de imágenes, como puede ser una videocámara.

Sin embargo, a este concepto lingüístico debemos imponerle unos límites para que sea considerado como un dato personal susceptible de protección por la legislación pertinente.

A este respecto, debemos decir que no cualquier imagen debe ser considerada como dato personal susceptible de protección pues, para que ésta sea considerada como tal, debe ofrecer un dato acerca de la persona a la que puede perjudicar.

Para conocer el significado de un dato, debemos dirigirnos al artículo 4 del Reglamento (UE) 2016/679[5] del Parlamento Europeo y del Consejo (en adelante RGPD), en especial, a su apartado 1, que define a los datos personales como *"toda información sobre una persona física identificada o identificable"*, entendiéndose por tal, cualquier persona que pueda ser identificada de forma directa o indirecta a través del tratamiento de estos datos, tal y como establece en su artículo 1 la Instrucción 1/2006[6] de la Agencia Española de Protección de Datos (en adelante AEPD).

[4] Enlace al concepto "imagen" que ofrece el diccionario de la Real Academia de la Lengua Española: https://dle.rae.es/?w=imagen

[5] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos. Enlace al documento: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[6] Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Enlace al documento: https://www.boe.es/buscar/act.php?id=BOE-A-2006-21648

Por ello, no podemos considerar como dato una imagen de una habitación vacía. Sin embargo, sí podrá considerarse como dato una imagen de esa misma habitación si una persona estuviese en ella.

Hay que tener en cuenta que la imagen, como dato, es muy importante para cada persona, pues es lo que puede diferenciarnos a unos de otros de una manera fácil, al igual que nuestra voz o nuestro nombre.

Por otro lado, en lo referente al movimiento de la imagen, diferenciaremos entre una imagen estática o puntual y una imagen en movimiento o continua, pues deberemos distinguir entre un sistema de videovigilancia y uno de videoseguridad.

Finalmente, tratando la imagen como un dato personal hemos de hacer referencia al Considerando 51 del RGPD, que establece que el tratamiento de fotografías no ha de considerarse como un tratamiento de categorías especiales de datos personales, salvo en el caso de las imágenes faciales, que se considerarán un dato biométrico a tenor del artículo 4, definición 14 del mismo Reglamento.

2.2. Derecho a la Intimidad y a la Propia Imagen.

Como ya se dijo al inicio de este apartado, el derecho a la Intimidad y a la propia Imagen se encuentran reconocidos por el artículo 18 CE, y están regulados por la Ley Orgánica 1/1982, de 5 de mayo, *de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*.

El derecho a la intimidad se encuentra estrechamente unido con otros derechos, tal y como establece la STC nº 110/1984[7], de 26 de noviembre, en su fundamento jurídico 3, que expone que la inviolabilidad del domicilio y de la correspondencia son libertades tradicionales en las que se reflejaba este derecho a la inviolabilidad.

Dentro del estudio que aquí se realiza, cabe hacer mención del artículo séptimo de la LO 1/1982, que establece que *"tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado en el artículo segundo de esta Ley: 1. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas"*.

[7] Sentencia del Tribunal Constitucional (Sala Primera) nº 110/1984, de 26 de noviembre. Ponente: Don Ángel Latorre Segura. Roj: RTC 1984\110.

Referente a la limitación del derecho a la intimidad, la Sentencia del Tribunal Constitucional nº 124/1999[8], de 15 de julio, establece en su fundamento jurídico 5 que el derecho a la intimidad *"tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y al conocimiento de terceros, sean estos poderes públicos o simpes particulares".*

Es ésta la postura que defiende la Sentencia del Tribunal Superior de Justicia de Andalucía número 1268/2017[9], de 5 de julio, en la que la Administración de Loterías nº7 de Málaga instaló un sistema de cámaras de videovigilancia sin informar debidamente a una de sus trabajadoras, la cual fue despedida. Esta trabajadora desconocía que estas cámaras grabasen de forma continua, de tal forma que aprovechó su conocimiento sobre claves y accesos al establecimiento para desconectar las alarmas y, así, evitar que *"las cámaras grabasen"*. Esto, junto con la finalidad para la que fueron instaladas las cámaras (seguridad del establecimiento), distinta a la de control laboral de los trabajadores, causó una intromisión en la intimidad de la trabajadora, pues estaba siendo grabada sin consentimiento, por lo que entraba de lleno en lo que el apartado 5 del artículo séptimo de la Ley Orgánica 1/1982 viene a describir como *"lugares o momentos de su vida privada"*.

A partir de estas delimitaciones, podemos observar que hay una parte de la vida de las personas que se encuentra protegida de ser conocida y divulgada frente al resto de la sociedad o de terceros individuales, y otra parte de la vida de las personas en las que, debido a su acción e interacción con los demás, prima el interés general y, por tanto, el derecho a la intimidad se ve restringido.

Esta postura se ve reflejada, como ya hemos hecho referencia anteriormente, en el apartado 5 del artículo séptimo de la LO 1/1982, que establece que se considera intromisión ilegítima la captación de imágenes de alguien *"en lugares o momentos de su vida privada"*. Así viene a reforzarlo la LO 3/2018[10], de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales* (en adelante LOPD-GDD), en su artículo 22.2 al permitir sistemas de seguridad en el exterior *"sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado"*.

[8] Sentencia del Tribunal Constitucional (Sala Primera) nº 124/1999, de 28 de junio. Ponente: Don Pablo Manuel Cachón Villar. Roj: RTC 1999\124

[9] Sentencia del Tribunal Superior de Justicia de Andalucía, Málaga (Sala de lo Social, Sección 1ª) nº 1268/2017, de 5 de julio. Ponente: Don Manuel Martín Hernández-Carrillo. Roj: AS 2017\2110

[10] Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales. Enlace al documento: https://www.boe.es/eli/es/lo/2018/12/05/3

Según el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea, "toda persona tiene derecho al respeto de su vida privada y familiar" y de su domicilio, ofreciendo la misma idea el artículo 8 del Convenio Europeo de Derechos Humanos en su apartado 1. Así se consolidaba esta protección hacia esa parte de la vida de las personas que sólo corresponde "disfrutar" a ellas.

Esto nos hace observar la gran fuerza que ha obtenido esta protección, llegando a ser uno de los derechos fundamentales de la Unión Europea.

Hay que recordar que este derecho a la intimidad personal y familiar y el derecho a la imagen tienen una gran relación, aunque tienen un contenido y objeto distinto. Así pues, el derecho a la propia imagen pretende otorgar el control de su aspecto físico a su titular, para que sea éste quien decida qué hacer con su imagen. Sin embargo, este control no es absoluto, pues el artículo octavo de la LO 1/1982 fija una serie de limitaciones, entre las que debemos destacar la captación de imágenes durante actos públicos o lugares abiertos al público de *"personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública"*. Esta limitación supone un sometimiento del interés personal al interés general.

Es en este punto donde podemos encontrar un caso bien conocido por todos como es el del intento de hurto por Cristina Cifuentes en un supermercado. A continuación, podrá encontrar un breve resumen de la investigación y sanción impuesta por la Agencia Española de Protección de Datos junto con la relación que pudiera tener este caso concreto con el derecho a la Intimidad y a la Propia Imagen de Cristina Cifuentes.

2.2.1. Caso práctico

El 25 de abril de 2018 se hicieron públicas, a través de distintos medios de comunicación, las imágenes captadas por las cámaras de videovigilancia instaladas en un supermercado. En ellas se podía observar cómo, la entonces diputada en la Asamblea de Madrid, Cristina Cifuentes[11] era conducida, en mayo de 2011, hasta un habitáculo por un trabajador de seguridad.

[11] Cristina Cifuentes es una política perteneciente al Partido Popular que llegó a ser la Presidenta de la Comunidad de Madrid. La Sra. Cifuentes había estudiado Derecho y su atracción por la política hizo que se incorporase a las filas de Alianza Popular en 1980. Tras años como asesora en este partido político, consiguió un escaño en la Asamblea de Madrid en 1991. En ese momento se iniciaría su carrera política en esta cámara regional, en la que desempeñaría distintos cargos a lo largo del tiempo.

Finalmente, fue elegida presidenta de la Comunidad de Madrid en junio de 2015, puesto del que dimitiría en abril de 2018.

Allí, Cristina Cifuentes, después de una extensa conversación, sacaba de su bolso personal dos productos que había sustraído. Estas imágenes fueron difundidas por los medios de comunicación, incluso, llegando a ser titular de algunas cadenas de televisión en franjas horarias de máxima audiencia.

La directora de la AEPD pone en funcionamiento una investigación para determinar si han sido afectados los datos personales de Cristina Cifuentes. Ello concluirá con la Resolución R/00423/2019 al Procedimiento nº PS/00336/2018[12] de la AEPD.

Para poner un poco en antecedentes, se ofrecen a continuación información del caso con testimonios del personal que intervino en los hechos y de los responsables. En este caso, era una empresa externa la encargada de la seguridad del establecimiento en cuestión.

El contrato suscrito por el supermercado destaca el siguiente contenido:

- El servicio objeto del contrato es la vigilancia de los establecimientos del supermercado, sin hacer mención individual de ellos.
- El apartado 15 del contrato establece que *"en aquellos casos en que el Contratista, directa o a través de sus empleados, pudiera tener acceso a Datos de Carácter Personal […], se obliga a "no comunicarlos ni cederlos y a mantener el carácter confidencial de los mismos, así como a adoptar y respetar las medidas organizativas, técnicas y de seguridad que la Propiedad estime necesarias""*.

Por su parte, el vigilante de seguridad manifiesta que sólo podía acceder al sistema de videovigilancia en tiempo real, por lo que no tenía acceso al almacenado de grabaciones. Además, éste desconocía quién debía ser la persona encargada de entregar las grabaciones a las Fuerzas y Cuerpos de Seguridad del Estado en este tipo de casos.

Por otro lado, el que ocupaba el cargo de Inspector de Servicios de Zona para la empresa externa de vigilancia reconoce al Director del Centro y Gerente como *"la persona autorizada para tratar las imágenes grabadas por el sistema de videovigilancia"*, *"que tenía en su despacho el ordenador con el programa para extraer las imágenes"*[13]. Este despacho, según las palabras del Director del Centro y Gerente, se

[12] Resolución R/00423/2019 al procedimiento nº PS/00336/2018 de la AEPD. Enlace al documento: https://www.aepd.es/es/documento/ps-00336-2018.pdf

[13] Palabras textuales otorgadas por el Inspector de Servicios de zona para CASESA a la investigación de la fuga de datos personales que afecta a Cristina Cifuentes y recogidas en la Resolución R/00423/2019.

encontraba *"cerrado con llave"*, pudiendo entrar en el despacho sólo él y la responsable de recursos humanos.

Atendiendo a los antecedentes descritos en el procedimiento antes mencionado, entre los que encontramos los anteriormente expuestos, la Agencia Española de Protección de Datos trata, en esta Resolución, de diferenciar al responsable del tratamiento y al encargado, utilizando para ello el artículo 3.d) de la LO 15/1999, de 13 de diciembre, *de Protección de Datos de Carácter Personal* (en adelante LOPD), que considera al responsable como la *"la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento"*, mientras que será encargado, de acuerdo con el apartado g) del mismo artículo, *"la persona física o jurídica, autoridad, servicio o cualquier otro organismo que, solo o juntamente con otros, trate datos personales por cuenta del responsable del tratamiento"*.

Por lo tanto, podemos decir que el responsable del tratamiento es aquella persona, física o jurídica, que pretende llevar a cabo un tratamiento de datos personales, para cuyo fin ha de fijar una serie de medidas que protejan esos datos a tratar.

Por su parte, el encargado del tratamiento es aquel que actúa por cuenta del responsable, siguiendo sus directrices, para tratar los datos objeto del tratamiento.

Para simplificar esta situación, se podría poner como ejemplo una situación cotidiana, como puede ser el de una empresa cuya labor de nóminas y contratación de personal lleva una gestoría. En este caso, la empresa es la responsable del tratamiento de los contratos de personal y del pago de las nóminas. Sin embargo, al no encontrarse cualificada para llevar a cabo esta tarea, acude a la gestoría para que realice dicha tarea, por lo que ésta última actuará como encargada del tratamiento.

Al igual que en este ejemplo ocurre en el caso que aquí tratamos con el control entre el supermercado y la empresa de vigilancia.

Además, hace referencia al artículo 12.3 LOPD, que obliga al encargado a destruir o devolver los datos obtenidos al responsable después de finalizar el contrato., mientras que su apartado 4 hace responsable del tratamiento al encargado cuando éste *"destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato"*.

Así pues, la AEPD considera que infringe el artículo 9 LOPD, puesto que no ha tomado las medidas necesarias para garantizar la seguridad de las grabaciones, y el artículo 4.1 LOPD, pues la empresa no estaba habilitada para tratar los datos de personas

que habían cometido delitos o faltas. Es por esto que la AEPD impone dos multas al supermercado dos multas. La primera por la infracción del artículo 9 LOPD, y la segunda por la infracción del artículo 4.1 LOPD.

Junto al tratamiento que acabamos de mostrar desde el punto de vista de la AEPD, podemos observar en este caso una apreciable intromisión en la intimidad de las personas.

Esto se debe a que, aun siendo un cargo público en el momento de la intención del hurto como en el de la publicación de las imágenes, Cristina Cifuentes se encontraba realizando tareas de su vida cotidiana como era hacer la compra en un supermercado, lo que viene a ser uno de esos *"lugares o momentos de su vida privada"* de los que hablábamos antes caracterizado por su cotidianeidad y su carácter personal que supone para cada uno de los individuos de la sociedad, de tal forma que se está difundiendo una grabación de seguridad de la vida privada de una personalidad pública, protegida por el Convenio Europeo de Derechos Humanos y otras normas aplicables como ya hemos tratado anteriormente.

A este respecto, hemos de decir que la transcendencia de este caso se debe, no a la importancia de los objetos sustraídos, sino a la persona que los había sustraído. Desde el primer momento en que se publican las imágenes, todos los medios de comunicación pretenden atraer la atención de la audiencia con el nombre de la persona que llevó a cabo dicha acción y utilizando la portada para darle más fuerza a la noticia. Debemos tener en cuenta que la imagen pública de Cristina Cifuentes acababa de verse afectada por falsedad documental en el Caso Máster[14], en el que se investigaba si Cristina Cifuentes había, o no, falsificado el acta del tribunal que debía examinarla de su Trabajo de Fin de Master (TFM).

Esto permitió a la prensa aprovechar la situación para minar más, si cabía, la moral de la susodicha. Su cargo como presidenta de la Comunidad de Madrid pendía de un hilo, y esta noticia podría ser el detonante de una dimisión inminente, de tal forma que la noticia copó las portadas de todos los periódicos de tirada regional y nacional[15], así como los noticieros de radios y televisiones.

[14] Enlace a noticia referente a la difícil situación que vivía Cristina Cifuentes en los días anteriores al hecho que aquí tratamos sobre el hurto producido en un supermercado: https://elpais.com/politica/2018/04/21/actualidad/1524329945_100589.html

[15] Portadas de diarios nacionales del día 26 de abril de 2018, día posterior al que se hicieron públicos los videos del hurto y de la dimisión de Cifuentes. Podemos apreciar en la portada de El Mundo cómo esta noticia *"remata"* a Cifuentes después del Caso Máster que la implicaba. Enlace: https://www.europapress.es/nacional/noticia-portadas-periodicos-hoy-jueves-26-abril-2018-20180426000046.html

Es por ello que podemos decir que la atención de los medios de comunicación era, precisamente, por ser un personaje público que estaba a la orden del día en la sociedad española por un escándalo académico. No obstante, el interés de los ciudadanos por un personaje público no debe invadir la esfera privada de la vida de éste.

Hemos de considerar que si ese intento de hurto lo hubiese realizado un ciudadano medio español no hubiera sido noticia en ningún medio de gran relevancia, pues la importancia de la acción es mínima, pero, en este caso, al tratarse de uno de los principales dirigentes de la geografía española, la importancia radica en el sujeto y no en la acción.

Además, y para finalizar, con la difusión de estas grabaciones, podemos observar ese daño al derecho a la propia imagen que protege a las personas, pues Cristina Cifuentes había perdido el control de su aspecto en su vida privada por una empresa que no puso las medidas necesarias para proteger los datos de las personas que aparecían en las grabaciones.

2.2.2. Intimidad vs Seguridad

Este es un gran debate que cada vez está más a la orden del día y que podrá observarse a lo largo del trabajo que aquí se expone, lo que ha hecho que exista una reiterada jurisprudencia nacional y supranacional acerca de este tema.

Lo cierto es que la grabación de nuestra vida diaria se entromete, aunque legalmente, de una forma muy agresiva en nuestras acciones rutinarias. Esto ha provocado que muchas personas rechacen estos sistemas de videovigilancia, pues consideran que son libres de elegir qué hacer y cómo hacerlo sin que nadie lo sepa.

Sin embargo, el fin de estas herramientas es la protección de las personas o bienes de éstas, y esto es lo que hace que haya otro tipo de personas que defienden la utilización de cámaras de videovigilancia. Esto se debe a que estas personas anteponen su seguridad y la de su patrimonio a la libertad y confidencialidad de sus acciones.

Por ello, la LO 1/1982 ha fijado, como ya dijimos anteriormente, la limitación de estas grabaciones de personas *"en lugares o momentos de su vida privada"*. Pero, atendiendo a la LOPD-GDD, podemos deducir de su artículo 22.2 que la vía pública podría incluirse en esos lugares de la vida privada de las personas a los que acabamos de referirnos, puesto que establece que *"sólo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible"* para preservar la seguridad de las personas y bienes.

Éste es el principal punto del conflicto que aquí planteamos pues, aunque nos sintamos acosados por un ejército de videocámaras instaladas en locales comerciales y

otros establecimientos, la vía pública constituye un espacio común en el que pueden ocurrir una gran cantidad y variedad de incidentes que, a nuestro juicio, deben ser grabados para proteger a las personas y sus bienes.

Es en esta idea en la que se basa nuestro pensamiento a la hora de considerar, en este caso, la primacía del interés general sobre el personal a la hora de grabar en la vía pública.

Si bien estas videocámaras son instaladas para proteger un determinado patrimonio individual, es cierto y necesario destacar que estas cámaras buscan, de un lado, proteger a la sociedad de aquellas personas que cometen una infracción, ofreciendo una prueba que permita castigar a los que cometiesen el delito concreto, y, de otro lado, proteger a las personas que, discurriendo por la vía pública, son víctimas de una lesión hacia sus derechos o integridad física. Es por ello que las videocámaras estarían cumpliendo con esa finalidad a la que hacíamos mención y que está establecida en el artículo 22.1 de la LOPD-GDD.

El ejemplo más claro de la seguridad que ofrecen los sistemas de videovigilancia está en Londres. Según el artículo *Londres, capital de la videovigilancia*[16] que publicaba el diario El País el 9 de agosto de 2011, eran cerca de 2.500 delincuentes los detenidos en 2010 en la capital inglesa gracias a la videovigilancia por circuito cerrado, con lo que se demuestra la importancia de la videovigilancia en la vía pública, la cual, a día de hoy, se encuentra fuertemente regulada y restringida en nuestro país.

3. GRABACIÓN DE VOZ VS GRABACIÓN DE LA IMAGEN

En este apartado trataremos de una forma breve la grabación de voz, pues aun siendo independiente de la grabación de imagen, en nuestra sociedad se encuentran estrechamente ligadas ambas acciones. Es por esto que le concedemos a la grabación de voz un pequeño epígrafe en nuestro trabajo.

Las personas solemos relacionar una imagen con un sonido. Este sonido nos permite hacer más clara una imagen, pudiendo obtener de ella más detalles. Sin embargo, este hecho, a la hora de realizar una grabación y tratar estos datos, es muy complejo, pues debemos basar nuestro tratamiento en los principios relativos a éste que fija el artículo 5 del Reglamento[17]. De acuerdo con este artículo, los datos han de ser *"limitados a lo necesario con los fines para los que son tratados"*.

[16] Enlace al artículo que aquí se trata desde el sitio web del diario El País: https://elpais.com/internacional/2011/08/09/actualidad/1312840806_850215.html

[17] Este término es utilizado con el fin de simplificar y hacer más fácil la lectura al lector en sustitución del Reglamento General de Protección de Datos o RGPD.

Por su parte, el artículo 25 del RGPD establece que será el responsable el que habrá de tomar las medidas necesarias para cumplir con los requisitos establecidos por el Reglamento, poniendo por ejemplo la minimización de datos, es decir, la utilización de datos mínimos para alcanzar la finalidad perseguida.

La AEPD ofrece un Informe Jurídico sobre la Grabación de Voz y Proporcionalidad[18] **(**Informe Jurídico 2017-0139 de la AEPD) en el que considera la grabación de voz como un tratamiento independiente al de grabación de la imagen, de tal forma que el que uno sea legítimo, no quiere decir que el otro lo sea.

Este informe, que nos servirá de ejemplo práctico en este tema, analiza una consulta realizada por parte de un ayuntamiento que pretende instalar un sistema de videovigilancia y grabación de voz con el que se va a obtener la imagen y voz de quienes accedan al edificio consistorial.

La consulta que aquí se trata proviene de un ayuntamiento que pretende instalar un sistema de videovigilancia para controlar la seguridad y los accesos a los edificios municipales y la asistencia de los empleados. Para ello pretende, a través de dicho sistema, grabar la imagen y la voz de todos aquellos ciudadanos que se encuentren en el edificio y de los trabajadores.

Para resolver la consulta que aquí se realiza, la AEPD se basa en el RGPD y en la Sentencia del Tribunal Constitucional 98/2000[19].

Tal y como comentábamos antes, la AEPD, sobre la instalación del sistema de videovigilancia en cuestión, informa que *"se deberá respetar el principio de proporcionalidad, valorando así la posibilidad de adoptar otros medios menos intrusivos a la intimidad de las personas"*. Esto nos lleva, por tanto, como ya decíamos, a la minimización de datos que establece el artículo 5 del Reglamento.

Atendiendo a esto, debemos decir que, si bien el sistema de videocámaras podría ser proporcional para conseguir el fin que se busca, que es el de seguridad y acceso a los edificios municipales y el control de asistencia de los empleados, el sistema de grabación de voz no lo sería. Esto se debe a que con la imagen captada de una persona entrando en el edificio nos bastaría para saber quién y cuándo ha entrado en la dependencia municipal, mientras que la voz no nos aportaría nada nuevo a la finalidad perseguida.

[18] Enlace del informe jurídico: https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-grabacion-de-imagenes-y-voz-proporcionalidad.pdf

[19] Sentencia del Tribunal Constitucional (Sala Primera) nº 98/2000, de 10 de abril. Ponente: Don Fernando Garrido Falla. Roj: RTC 2000\98

Así lo hace ver la AEPD al considerar que *"el hecho de que pueda resultar legítima la videovigilancia por razones de seguridad, no implica necesariamente que se legitime la grabación de la voz",* añadiendo que estaríamos ante un tratamiento de datos distinto.

Por otro lado, la STC 98/2000, que sirve de base para la decisión de la Agencia Española de Protección de Datos, trata el caso de una empresa que pretendía controlar la actividad de sus trabajadores en sus instalaciones. Para ello, junto al sistema de videovigilancia que ya estaba instalado, fija un nuevo sistema de grabación de voz con el fin de poder obtener pruebas audibles de las posibles reclamaciones realizadas por los clientes.

En este caso, el Tribunal Constitucional hace referencia a la STC 57/1994[20], en la que se establece que *"el derecho a la intimidad no es absoluto"*, por lo que quedaría limitado por el poder de dirección del empresario, pero éste, a su vez, ha de realizarse, de acuerdo con el artículo 20.3 de la Ley del Estatuto de los Trabajadores[21] (en adelante LET), *"guardando en su adopción y aplicación la consideración debida a su dignidad* (del trabajador)*"*. Esto se justifica, tal y como establece el artículo 4.2e) LET, con que los trabajadores tienen derecho *"al respeto de su intimidad y a la consideración debida a su dignidad"*. A ello, el Tribunal Constitucional añade que *"la mera utilidad o conveniencia para la empresa no legitima sin más la instalación de los aparatos de audición y grabación"*, pues ésta ya contaba con el sistema de videovigilancia, el cual era suficiente para conseguir la finalidad buscada.

Así, el Tribunal Constitucional considera que la instalación de micrófonos no es proporcional para la finalidad perseguida, mientras que la grabación de imágenes sí lo es. Por tanto, podemos observar en este caso esa diferenciación de la que hablábamos antes entre la grabación de imagen y voz como distintos tratamientos de datos.

Por lo tanto, la decisión de la AEPD ante esta consulta realizada, basándose en lo anteriormente expuesto, es la de considerar desproporcionada la medida de instalar un sistema de grabación de voz para esa medida, pues se van a realizar *"grabaciones indiscriminadas de voz y conversaciones de los empleados y público en general que acceden a los edificios del Ayuntamiento*", y esto va a conllevar un gran sacrificio del derecho a la intimidad de las personas que están siendo grabadas.

[20] Sentencia del Tribunal Constitucional nº 57/1994, de 28 de febrero. Ponente: Don Julio Diego González Campos. Roj: RTC 1994\57

[21] Real Decreto 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. Enlace al documento: https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430

4. SEÑALIZACIÓN DE ZONA VIDEOVIGILADA

En este apartado trataremos una de las limitaciones técnicas más básicas en la videovigilancia como es el deber de informar, que se materializa en la señalización de la zona que va a ser controlada por cámaras. Este va a ser el tema que trataremos en este epígrafe.

La señalización de zona videovigilada es la medida más extendida en la actualidad para dar por cumplido el deber de información establecido en el artículo 12 del RGPD, por el que el responsable del tratamiento deberá tomar *"las medidas oportunas para facilitar al interesado toda la información indicada en los artículos 13 y 14"*.

Esta normativa establece que la información que hay que indicar en este sentido es: la identidad y los datos de contacto del responsable, los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento, el plazo durante el que se conservarán los datos personales o el derecho a presentar una reclamación ante la autoridad de control competente.

Por su parte, la LOPD-GDD hace referencia, en el apartado 4 de su artículo 22, al artículo 12 antes mencionado, considerando que un cartel informativo es suficiente para dar por cumplido ese deber de información. Sin embargo, este cartel no puede estar en cualquier sitio, sino que, tal y como dice la LOPD-GDD, ha de estar "en lugar suficientemente visible". La Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, establece en su artículo 3, de igual forma, que el responsable debe cumplir el deber de información colocando, al menos, un cartel informativo en las zonas videovigiladas de forma visible.

Sin embargo, ninguna apreciación hace la norma acerca de qué ha de entenderse por un *"lugar suficientemente visible"*.

A este efecto, el Informe Jurídico de la AEPD sobre Dimensiones del Cartel de Videovigilancia[22] nos ofrece unas precisiones acerca de las dimensiones y posicionamiento del cartel informativo de zona videovigilada.

Según este Informe Jurídico, no hay unas medidas mínimas establecidas por la AEPD, por lo que éste ha de ser *"acorde con el espacio en el que se vaya a ubicar"*. Así

[22] Informe Jurídico de la AEPD sobre Dimensiones del Cartel de Videovigilancia. Enlace al documento: https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-dimensiones-cartel-videovigilancia.pdf

pues, el cartel fijado en un tren o un autobús será menor que el establecido en un hipermercado.

Por otro lado, en lo referente al lugar donde estará ubicado el cartel, el Informe Jurídico aquí tratado considera que *"no es necesario que se coloque debajo de la cámara"*, sino que bastará con que se fije en la entrada del mismo. Así lo ofrece la AEPD también en la Guía sobre el uso de videocámaras para seguridad y otras finalidades[23] publicada en el sitio web www.aepd.es.

Sin embargo, es muy frecuente ver este tipo de carteles dentro de los locales, pero esto no es correcto.

4.1. Objetivo del cartel informativo.

La principal y verdadera función del cartel informativo de zona videovigilada no es otro que la obtención del consentimiento por parte de aquel del que se va a obtener su imagen, pues sin este consentimiento no podría ser tratada su imagen.

Esto se debe a la licitud del tratamiento que establece el artículo 6 del RGPD y que traspone la LOPD-GDD en su artículo 6. De acuerdo con el artículo 6 del RGPD, el tratamiento de datos es sólo lícito cuando *"el interesado dio su consentimiento para el tratamiento de sus datos personales"*, de tal forma que el interesado debe consentir su grabación antes de que ésta se realice.

Lo más normal para recabar el consentimiento del interesado es entregar un documento en el que éste dé sus datos y firme, pero a nadie se le escapa la dificultad de tener que firmar un documento cada vez que se entra a un local comercial, una cafetería, un parking o un supermercado. Igual ocurre al plantearnos si, como empresarios de ese local, deberíamos apagar las cámaras si una persona no consintiera dicho tratamiento.

Con el objetivo de hacer más amena nuestra vida y facilitar la instalación de sistemas de videovigilancia en zonas de acceso al público, el RGPD y la LOPD-GDD prevén un consentimiento ni escrito ni verbal, sino conductual.

Para entender qué es el consentimiento del interesado, debemos dirigirnos al concepto 11 que nos ofrece el artículo 4 del RGPD, que establece que es *"toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"*.

[23] Guía sobre el uso de videocámaras para seguridad y otras finalidades, publicada por la AEPD. Enlace: https://www.aepd.es/sites/default/files/2019-09/guia-videovigilancia.pdf

Junto a esto, el Considerando número 32 del RGPD nos hace ver que, cuando el consentimiento se otorgue mediante acto afirmativo, éste ha de ser claro, de tal forma que podamos observar, sin equivocación alguna, ese deseo del interesado de permitir el tratamiento de sus datos.

Por lo tanto, al colocarse este cartel junto a la entrada de la zona videovigilada y, por consiguiente, informar al interesado, se está intentando recabar el consentimiento del interesado para tratar sus datos a través del sistema de seguridad instalado. De esta forma, el interesado estaría otorgando su consentimiento al entrar en esa zona videovigilada, pues es ésta la acción afirmativa, libre y clara de la que hablábamos por la que puede obtenerse el consentimiento.

Una vez ha entrado el interesado en la zona videovigilada, podrá ejercer los derechos que el RGPD reconoce entre los artículos 15 y 22, aunque el tratamiento de la imagen ya realizado sí será lícito, pues ya se dio el consentimiento antes del inicio del tratamiento, tal y como refleja el artículo 13.2 c) al referirse al derecho de retirar el consentimiento que se otorga al interesado para su protección.

Es por esta razón por la que el cartel ha de estar en la entrada de la zona que va a ser videovigilada, pero, ¿qué ocurre en el caso de que el interesado tenga una discapacidad visual severa?

Este caso puede llegar a ser muy complejo, pues, si se tratase de una persona ciega, estaríamos ante un tratamiento ilícito, ya que no se ha informado (mediante el cartel informativo) de que va a entrar en una zona videovigilancia. Por lo tanto, el responsable del tratamiento, antes de que sea tratada la imagen de esta persona, ha de informarle por otro medio del tratamiento que se va a realizar. Así nos lo da a razonar la Guía Para El Cumplimiento Del Deber De Informar[24], al considerar que, al ser distintos los procedimientos de recogida de información, *"los modos de informar a las personas interesadas deben adaptarse a las circunstancias de cada uno de los medios empleados para la recopilación"*.

El deber de información, para el caso aquí tratado, debería realizarse de forma verbal o escrita (en braille), pues un cartel que ha de ser visto no sería válido para obtener el consentimiento de aquel que no cuenta con una capacidad visual suficiente para distinguir el cartel identificativo. Sin embargo, a día de hoy, no es usual ver este tipo de comportamientos en nuestra sociedad.

[24] Guía para el cumplimiento del deber de informar, publicada por la AEPD. Enlace: https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf

Otro caso semejante es el de aquellas personas que no hablan español o que, simplemente, son iletradas, es decir, analfabetas.

En esta ocasión, el responsable del tratamiento no puede apreciar si la persona que entra en la zona controlada por cámaras cuenta con una anomalía que le impide conocer del tratamiento que se va a llevar a cabo de su cámara.

Para este tipo de circunstancias, al igual que para el caso de una persona con una deficiencia visual leve, aunque nada establece la Instrucción 1/2006 de la AEPD, el cartel identificativo al que ésta hace referencia y que ofrece la AEPD sí incluye un icono de una cámara de seguridad.

Con este icono se permite dar una información muy básica sobre el tratamiento que se está realizando en dicho lugar. De esta forma, aquella persona que no conozca nuestro idioma o no sepa leer podrá evitar el tratamiento y así, el responsable no estará llevando a cabo un tratamiento de datos personales ilícito.

Así, una vez la persona en cuestión haya observado dicho icono, antes de entrar en la zona videovigilada, podrá solicitar información acerca del tratamiento de videovigilancia al personal que se encuentre subordinado al responsable, con lo que se daría por cumplido el deber de información hacia el interesado.

No obstante, si nos encontráramos ante un cartel informativo que no contase con un icono de esta categoría no podríamos decir que se haya cumplido el deber del que ya hemos hablado y, por tanto, el tratamiento respecto a esa persona sería ilícito.

4.2. Diseño y contenido del cartel.

En este subapartado trataremos el contenido y el diseño del cartel identificativo que informa de una zona se encuentra videovigilada y que se tratarán los datos de imagen de las personas que accedan a ella.

Es cierto que con el cartel se pretende informar del tratamiento de imágenes obtenidas de personas, pero, ¿sirve cualquier cartel para cumplir con el deber de información?

Atendiendo al ANEXO de la Instrucción 1/2006 de la AEPD, este cartel debe incluir como contenido:

- Referencia a la Ley Orgánica 15/1999, aunque, al está derogada, deberá hacerse referencia a la legislación vigente en ese momento, es decir, al RGPD o a la LOPD-GDD.
- Identificación del responsable ante el que pueden ejercerse los derechos establecidos entre los artículos 15 y 22 RGPD.
- Posibilidad de ejercer los derechos articulados en el RGPD.

A continuación, este mismo anexo ofrece como modelo el que facilita la Agencia Española de Protección de Datos[25], el cual se caracteriza por un icono de una cámara de videovigilancia y el contraste de letras en color negro y el fondo en amarillo, de tal forma que este cartel se hace llamativo para llamar la atención de quien vaya a acceder a la zona videovigilada.

Sin embargo, no encontramos en la legislación vigente la obligación de utilizar el cartel que la AEPD nos ofrece, por lo que podemos concluir que sirve cualquier tipo de cartel siempre y cuando incluya los datos que más arriba hemos enumerado.

5. LIMITACIONES TEMPORALES EN LA VIDEOVIGILANCIA

Este epígrafe está dirigido a la limitación temporal de aquellas imágenes que han sido obtenidas a través de sistemas de videovigilancia, lo cual supone un límite temporal al tratamiento de datos fotográficos.

Esta limitación se deduce del artículo 17 del RGPD, referente al derecho de supresión que asiste a los interesados, por el que el responsable quedará obligado a suprimir los datos personales obtenidos y/o tratados cuando éstos *"ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados"*, o *"deban suprimirse para el cumplimiento de una obligación legal"*.

Respecto a la primera opción, recogida en el apartado a) del artículo antes mencionado, hay que considerar que, si el sistema de videovigilancia en cuestión se ha fijado para la protección de las personas u objetos o la asistencia al trabajo, su función es identificar quién ha realizado una infracción penal o administrativa o ha incumplido su contrato. De esta forma, una vez se ha podido comprobar que no ha ocurrido nada contra lo que pudiera utilizarse los datos obtenidos a través del sistema, éstos han de ser suprimidos, pues no son necesarios ya para ese fin, ya que no nos valdrán para comprobar quien cometerá una infracción o incumplimiento en el futuro.

Por otra parte, la segunda opción, que se encuentra protegida por el apartado e) del artículo 17 del RGPD, la cual se encuentra reflejada, como veremos a continuación, en la LOPD-GDD. Esta obligación legal pretende obligar a los responsables de los tratamientos a eliminar aquellos datos obtenidos y/o tratados aun cuando puedan seguir siendo útiles para estos.

[25] Cartel identificativo de zona videovigilada que ofrece la AEPD en su sitio web para su colocación una vez se haya rellenado. Enlace: https://www.aepd.es/sites/default/files/2019-09/cartel-videovigilancia.pdf

Esto supone una protección a los interesados que, no pudiendo solicitar la supresión de los datos que han sido recogidos por no cumplirse alguna de las demás circunstancias que recoge este precepto, quieren mantener su confidencialidad y poder sobre éstos.

Como acabamos de comentar, el artículo 22 de la LOPD-GDD establece la obligación de suprimir las imágenes captadas mediante un sistema de videovigilancia *"en el plazo máximo de un mes desde su captación"*. Esta limitación, como podemos observar, ofrece un amplio lapso de tiempo, el cual permite tener una importante capacidad de reacción ante hechos inapreciables en el día a día pero que afectan a aquellos elementos que constituyen el fin para el que fueron instaladas las cámaras de videovigilancia en cuestión.

Así, por ejemplo, podríamos estar ante el caso de un hurto continuado de dinero o mercancía por parte de un empleado, como ya veremos en otro apartado posterior, en el que no se aprecia la desaparición en un momento adecuado, pero a largo plazo sí, y esto sólo podremos observarlo y demostrarlo a través de las imágenes captadas día a día por las cámaras instaladas.

Hay que decir que, para este tipo de casos, la LOPD-GDD y el RGPD prevén una limitación a este derecho de supresión. Así, el RGPD establece en el apartado 1 del artículo 23 la limitación de los derechos que asisten a los interesados, siempre y cuando no se vea afectada la parte esencial de sus derechos y libertades fundamentales, cuando se busque salvaguardar, entre otras cosas, la seguridad pública, la ejecución de demandas civiles o *"la prevención, investigación, detección o enjuiciamiento de infracciones penales"*.

Esta misma idea es recogida por la LOPD-GDD en el apartado 3 del artículo 22 que, junto a ese límite de un mes del que hablábamos antes, reconoce una excepción por la que los datos *"hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de las personas, bienes o instalaciones*". Esta excepción permitirá a las Fuerzas y Cuerpos de Seguridad del Estado descubrir al autor de estos actos y, a los órganos judiciales competentes, llevar a cabo su actividad.

Para que esto se produzca, es necesario, como es evidente, entregar estos datos a la autoridad competente, tal y como establece el precepto ya mencionado, en el *"plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación"*, por lo que se genera una obligación de cooperación con las autoridades para encontrar al infractor.

Por lo tanto, este tratamiento de las imágenes ya no estaría basado en el apartado a) del artículo 6 del Reglamento, sino que pasaría a estar basado en el apartado c) del mismo artículo, por el que el tratamiento es lícito por ser *"necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento"* o, incluso, podría estar basado en el apartado d), que considera lícito el tratamiento cuando es *"necesario para proteger los intereses del interesado o de otra persona física"* en determinados casos de salud.

6. LA VIDEOVIGILANCIA EN EL ÁMBITO LABORAL

En este apartado se tratarán diversos casos reales a través de sentencias con los que se podrán observar diversos límites de la videovigilancia dentro de los centros de trabajo. Hay que decir que el ámbito laboral es el que cuenta con una mayor regulación y jurisprudencia en lo que respecta a videovigilancia, lo que hace que ésta se encuentre muy limitada en la empresa.

Por otro lado, en este apartado no se tratará de forma principal, como en los anteriores, la seguridad como fin de la videovigilancia, sino el control de los trabajadores en su puesto como una medida que facilita el poder de dirección y control del empresario.

Pero antes de analizar diversos casos de controversia en la videovigilancia del puesto de trabajo, vamos a hacer énfasis en el control empresarial ejercido a través de la videovigilancia.

Este poder de dirección y control de la actividad laboral se encuentra regulado en el artículo 20 de LET, cuyo apartado 3 establece que *"el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales"*, lo que podrá hacer a través de sistemas de videovigilancia. Sin embargo, este poder de dirección y control nunca podrá afectar a la intimidad y a la dignidad de los trabajadores. Así lo establece el artículo 18 de LET al defender que *"se respetará al máximo la dignidad e intimidad de los trabajadores"*.

Por su parte, el artículo 89 de la LOPD-GDD reconoce en su apartado primero al empleador el derecho a *"tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores"*.

De esta forma, podemos observar la superioridad del empleador consolidada por la legislación sobre los empleados, defendiendo así el interés último de la empresa frente al derecho de a la intimidad de los trabajadores en el centro de trabajo. Sin embargo, este mismo precepto trata de limitar este poder prohibiendo la instalación de este tipo de herramientas o instrumentos en *"lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos"* y, además, obligando al empleador a informar previamente a los empleados de dicho tratamiento.

En el lado opuesto, observamos que el segundo párrafo del artículo 89.1 LOPD-GDD refuerza el poder de control del empleador en este ámbito al considerar que *"se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo"* informativo del que ya hablamos en el caso de que se haya captado la comisión de un delito por parte de los trabajadores.

No obstante, *"la línea que separa dónde termina el poder del empresario y dónde comienza el derecho del trabajador a preservar su intimidad, es muy estrecha"*[26], por lo que depende de muchos factores que estemos ante una medida desproporcionada o no. Es por ello por lo que debemos tener en cuenta factores como el momento, el lugar o las personas que son grabadas con estos sistemas que tienen como fin el control laboral.

Atendiendo a esto, procederemos ahora a tratar uno de los actos que más relevancia tiene en nuestro país relativo la videovigilancia en el centro de trabajo. Tal es el caso de López Ribalda y otros contra el Reino de España.

6.1. Caso López Ribalda y otros contra el Reino de España

Relacionado con la información de zona videovigilada encontramos el Caso de López Ribalda[27], en el que el empleador de un pequeño supermercado, observando desajustes en las existencias del inventario y en las ventas del establecimiento, decide instalar un sistema de videovigilancia.

Dicho sistema de videovigilancia podía dividirse o diferenciarse en dos grupos de cámaras de distintos tipos. El primer grupo estaba conformado por cámaras estándares fijas de videovigilancia que enfocaban las entradas y salidas del establecimiento. Por su

[26] Mella Méndez, Lourdes y otros (2017), *Nuevas tecnologías y nuevas maneras de trabajar: Estudios desde el Derecho Español y comparado*, "Capítulo IX: El control empresarial a través de medios de videovigilancia", Madrid, Dykinson, páginas 215-228)

[27] Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) nº 144/2019, de 17 de octubre. Caso López Ribalda y otros contra España. Roj: TEDH 2019\144. Enlace a la sentencia (versión en inglés): https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-197098%22]}

parte, el segundo grupo estaba constituido por una serie de cámaras ocultas que grababan los puestos de trabajo de los trabajadores en las cajas registradoras.

El empleador informa a los trabajadores del sistema de videovigilancia visible y de su finalidad, que era la de evitar los robos que estaban ocurriendo. Sin embargo, no informa de las cámaras ocultas que acababa de instalar junto a las otras y que enfocaba a los puestos de trabajo de los trabajadores.

Una vez se accedió a las imágenes grabadas y se conoció quién estaba robando, el empleador reunió a las cinco mujeres que cometieron los delitos en su despacho, junto con una representante sindical y a la representante legal de la empresa. En esa reunión se les informó de los acontecimientos, mostrándoles las imágenes captadas y ofreciéndoles un acuerdo transaccional por el que se comprometían a no demandar a su empleador por despido improcedente a cambio de que éste no las denunciaría por robo.

Algunas de ellas no aceptaron estos acuerdos y optaron por demandar al empleador por despido improcedente, a las que se le unieron el resto que ya habían firmado los acuerdos. Dos de las demandantes se opusieron a la videovigilancia oculta, pues se había restringido su derecho a la intimidad. Por su parte, las otras tres demandantes alegaban coacción en la firma del acuerdo transaccional, pues iban a ser denunciadas si demandaban al empleador por despido improcedente.

Ante los tribunales españoles, esta medida de control se ajustaba a lo dispuesto en el artículo 20 de LET, que permite al empleador o empresario, en su apartado 3, tomar las medidas oportunas para controlar que los trabajadores cumplan con sus obligaciones. En lo referente a los acuerdos transaccionales, los tribunales consideraron que no podía demostrarse la existencia de coacción en la firma, pues las demandantes firmaron para evitar consecuencias penales y, además, hubo empleadas que se negaron a firmarlos.

Así pues, como la firma de estos acuerdos hizo procedentes los despidos, no fue necesario analizar los videos que algunas de las demandantes impugnaron.

Una vez tomada la misma decisión por los tribunales españoles a los que apelaron las demandantes, decidieron acudir al Tribunal Europeo de Derechos Humanos (en adelante TEDH) contra España, de cuyo caso conocería la Sección Tercera en Sala en un primer momento y, posteriormente, la Gran Sala del TEDH.

En este caso, las demandantes alegaron que este sistema de videovigilancia oculta había afectado a su derecho a la intimidad y que los órganos judiciales españoles no habían evitado el daño causado por estos videos al derecho antes mencionado. Por ello, basaron su alegación en el artículo 8 del Convenio para la Protección de los Derechos

Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, que establece en su apartado 1 que *"toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia"*. A este apartado se le une el segundo, que señala que *"no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho"*.

De esta forma, las demandantes alegaron que no se les informó de que iban a ser grabadas, tal y como establecía la legislación vigente, y, además, éstas consideraron que las grabaciones habían constituido la principal prueba en los procesos judiciales que habían tenido lugar.

Por su parte, el Gobierno de España señaló que nada tenía que ver en el caso, pues este sistema fue instalado por una empresa privada. Además, el gobierno informó que *"la legislación vigente en ese momento ofrecía a cualquier ciudadano la posibilidad de denunciar ante la Agencia de Protección de Datos el uso de videovigilancia encubierta"*, por lo que las demandantes tuvieron la oportunidad de alegar la falta de información que acusaba este sistema.

Ante esta alegación, el Tribunal Europeo, en su Sección Tercera, consideró que el término "vida privada" que se incluye en el artículo 8 del Convenio podría extenderse a *"actividades de carácter profesional o empresarial*", lo que da pie a una infracción del derecho a la intimidad de las demandantes. Esto se debe a que dichas cámaras podrían haber captado conductas personales realizadas por las demandantes en el puesto de trabajo, un lugar en el que están obligadas a estar por un contrato de trabajo.

En lo que se refiere a la proporcionalidad de la medida, la Sección Tercera del TEDH reconoce que el empresario *"no cumplió la obligación de informar"* sobre el sistema de videovigilancia oculta. Sobre este tema, expone un caso similar en el que se dio la razón al empresario. Este es el Caso Köpke[28], en el que el sistema de grabación oculta estaba motivado por una sospecha previa contra los trabajadores y, por tanto, se dirigió específicamente sobre determinados sujetos, hecho que no ocurría en el caso que aquí tratamos.

[28] Enlace a la decisión del TEDH (versión en inglés): https://hudoc.echr.coe.int/spa#{%22docname%22:[%22k%C3%B6pke%22],%22documentcollectionid2%22:[%22JUDGMENTS%22,%22DECISIONS%22,%22RESOLUTIONS%22],%22itemid%22:[%22001-101536%22]}

Es por ello que el tribunal consideró desproporcionada la medida e hizo ver que podrían haberse protegido los derechos del empresario de una forma menos intrusiva para el derecho a la intimidad de las demandantes.

En lo que se refiere a la indefensión producida por los videos obtenidos de forma ilícita para las demandantes, el Tribunal consideró que las demandantes *"tuvieron ocasión de impugnar la autenticidad y utilización"* de éstos. Además, éstos no constituyeron la única prueba en el juicio, sino que se presentaron otras pruebas que consolidaban los hechos.

Por lo tanto, a modo de conclusión, el Tribunal dictaminó a través de la STEDH 2018\1[29] que, si bien el uso de cámaras de videovigilancia en estas circunstancias es lícito como parte del poder de control que ostenta el empresario, es necesario que se cumpla con el deber de información, pues se está afectando al derecho a la intimidad de los trabajadores. Por lo tanto, en el caso que aquí tratamos, el tratamiento sería ilícito por una falta de información, lo que da lugar a una infracción en el derecho a la intimidad y a la imposibilidad, por parte de los trabajadores que son grabados, a ejercer los derechos que les reconocía en su momento la LOPD.

Ante esta decisión, el Gobierno de España solicitó que el caso pasase a ser tratado por la Gran Sala del Tribunal Europeo de Derechos Humanos.

Ya elevado el asunto a este órgano, las demandantes persisten en su posición de que se ha vulnerado el artículo 8 del Convenio al negarse los órganos jurisdiccionales españoles a anular el despido ante la utilización de las grabaciones obtenidas sin informar a éstas.

Frente a esta posición, el Gobierno mantiene que las demandantes tuvieron la oportunidad de acudir a la AEPD y de denunciar la conducta ante los tribunales por una posible violación de su derecho a la vida privada.

A este respecto, se pronuncia el tribunal dando cuenta de que el lugar que se grababa era establecimiento abierto al público, por lo que las acciones realizadas por las trabajadoras durante el tiempo en que las cámaras grabaron no podían ser consideradas como íntimas.

[29] Sentencia del Tribunal Europeo de Derechos Humanos nº 2018\1, de 9 de enero, iniciada por las demandas nº 1874/13 y 8567/13. Enlace al documento: https://www.mjusticia.gob.es/cs/Satellite/Portal/1292429076136?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Grupo&blobheadervalue1=attachment%3B+filename%3DSentencia_L%C3%93PEZ_RIBALDA__Y_OTROS_v_ESPA%C3%91A.pdf&blobheadervalue2=Docs_TEDH

Por otro lado, referente al artículo 8 del Convenio, el TEDH declara que dicho precepto obliga a los Estados a adoptar *"un marco legislativo que proteja el derecho en causa"*. Hecho este que sí se había producido por parte de España con la elaboración de la LOPD.

En lo que respecta a la proporcionalidad de la videovigilancia en el puesto de trabajo, el Tribunal estableció una serie de elementos a tener en cuenta para medir la proporcionalidad de esta medida. Éstos son:

- Información dada al empleado sobre las medidas a adoptar.
- Alcance de la vigilancia y conflicto con el derecho a la intimidad.
- Justificación el uso de la vigilancia.
- Posibilidad de usar medios menos lesivos.
- Consecuencias de la vigilancia.
- Garantías dadas al empleado.

Atendiendo a estos elementos, los tribunales españoles pudieron, a lo largo del proceso, considerar proporcionada la medida adoptada por el empresario para proteger su patrimonio.

De esta manera, la proporcionalidad observada por los órganos jurisdiccionales españoles junto con la legislación establecida por España para garantizar la protección del derecho a la intimidad a las trabajadoras, hacen que el TEDH considere que el artículo 8 del Convenio no se haya incumplido por parte de España. Esto se debe a que las trabajadoras pudieron iniciar un proceso contra la empresa privada para denunciar la infracción que ésta había cometido y poder, así, obtener una indemnización por el daño sufrido.

Por otro lado, este tribunal considera que no fueron las grabaciones las únicas pruebas que se utilizaron para dictaminar el despido como procedente.

Por lo tanto, una vez analizadas las circunstancias en las que se produjeron los hechos y las consecuencias que éstas han tenido, el Tribunal Europeo de Derechos Humanos, reunido en su Gran Sala, dictaminó en su sentencia nº 2019\144, a 17 de octubre de 2019, que no se había producido una infracción del artículo 8 del Convenio por parte del Reino de España.

Con este caso, podemos observar que la importancia del deber de información acerca del tratamiento de datos personales no es absoluto, sino que hay que tener también en cuenta, entre otras cosas, los intereses que se protegen por la medida de vigilancia en cuestión.

Debemos observar que, con esta sentencia del TEDH se hace más amplia la línea de nuestra jurisprudencia nacional a favor de la facultad que otorga el artículo 20 de LET al empleador para controlar la actividad de sus trabajadores.

Algunas de las sentencias del Tribunal Constitucional que siguen esta línea y que sirven de referencia a día de hoy para nuestros órganos jurisdiccionales son tenidas en cuenta por el TEDH y las tratamos a continuación.

6.2. Cajero captado por las cámaras

Sentencia del Tribunal Constitucional nº 186/2000[30].

Este es un caso que sigue la línea del tema del caso que acabamos de tratar. Hay que decir que esta sentencia ha permitido asentar una jurisprudencia casi unánime y el establecimiento de ciertos límites a la intimidad de los trabajadores en su puesto de trabajo en pro del poder de control con el que cuenta el empleador o empresario. Ésta es una sentencia que, a pesar de su antigüedad, sirve en muchos casos actuales como referencia en este tema.

En este sentido, debemos decir que los cambios en el ámbito laboral han sido mínimos durante este siglo, lo que ha permitido mantener vigente esta sentencia en el ámbito que aquí tratamos.

En esta ocasión, al igual que en la anterior, el empleador observa un desajuste de las cuentas del establecimiento. Ante esta situación, y la sospecha que recaía sobre el que actúa como recurrente ante el Tribunal que aquí resuelve, se opta por la instalación de un sistema de seguridad de circuito cerrado de televisión que permita captar las imágenes de las cajas registradoras en las que pudiera actuar el sujeto.

Las imágenes captadas permitieron observar que el actor se había apropiado, en diversos momentos, de dinero que se encontraba en la caja. También pudo apreciarse que otros dos cajeros se apropiaron de algunos productos desprecintados de bajo valor.

De acuerdo con esto, el recurrente presenta una demanda de amparo que fundamenta en la infracción de su derecho a la intimidad y a su imagen. Así pues, el recurrente considera nula de pleno derecho la prueba que constituían las grabaciones de video que presentó la empresa, pues ésta se ha *"obtenido vulnerando derechos fundamentales del trabajador".* Para ello, el recurrente se basa en el artículo 90.1 de la ya derogada Ley de

[30] Sentencia del Tribunal Constitucional (Sala Primera) nº 186/2000, de 10 de julio. Ponente: Don Fernando Garrido Falla. Roj: RTC 2000\186.

Procedimiento Laboral[31], que establecía que las partes procesales podían utilizar a su favor de pruebas de imagen y sonido *"salvo que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales"*.

Para ello, fundamenta su posición en que estas cámaras, que buscaban controlar el trabajo, también *"registran el resto de actos del trabajador pertenecientes a su intimidad"*, puesto que se trataba de una grabación continua del puesto de trabajo.

Por su parte, el tribunal hace referencia a la jurisprudencia por él asentada en la que considera que *"el derecho a la intimidad no es absoluto"*, aunque sí implica *"la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás"*. Además, el tribunal hace referencia al artículo 20 de LET, por el que se reconoce al empresario la facultad para tomar medidas que permitan controlar el rendimiento de sus trabajadores.

Sin embargo, el control del empresario, tal y como reconoce la sentencia posteriormente, no puede afectar de forma ilegítima a los derechos fundamentales de sus trabajadores, siendo en este caso afectado el derecho a la intimidad de los empleados en el centro de trabajo. Así pues, como después mostraría la sentencia, la instalación de estas cámaras tiene un resultado inconstitucional.

También podemos observar en esta sentencia el análisis que el Tribunal hace del circuito cerrado de televisión instalado por la empresa, deduciéndose que es una medida:

- **justificada**, pues se sospechaba del recurrente como causante de las irregularidades que sufría la empresa,
- **idónea para la finalidad perseguida**,
- **necesaria**, debido a que las grabaciones constituirían una prueba fundamental para demostrar los hechos, y
- **equilibrada**, pues únicamente se captaba la imagen de la zona en que trabajaba el sospechoso y en un tiempo limitado que permitiese corroborar las sospechas.

Por ello, el Tribunal considera que *"la intimidad del recurrente no resulta agredida"*, pues se trata de una medida necesaria para fundar las sospechas que la empresa tenía hacia él. Además, la empresa sólo pretendía, con estas grabaciones, conocer cuál era su comportamiento en el puesto de trabajo.

[31] Real Decreto Legislativo 2/1995, de 7 de abril, por el que se aprueba el texto refundido de la Ley de Procedimiento Laboral. Enlace al documento: https://www.boe.es/buscar/act.php?id=BOE-A-1995-8758&b=134&tn=1&p=19950411#a90

Finalmente, atendiendo al análisis que el Tribunal hace del sistema de grabación como medida para el control y vigilancia de los trabajadores por parte de la empresa, éste considera que *"los derechos a la intimidad personal y a la propia imagen, garantizados por el art. 18.1 CE, no han resultado vulnerados"*, por lo que desestima el recurso de amparo que el recurrente interpuso ante el Tribunal Constitucional.

Así pues, a diferencia del caso anterior, las cámaras de videovigilancia sólo se dirigen hacia un trabajador, no hacia toda la plantilla de trabajadores. Por tanto, en esta ocasión, podemos observar que no es necesario cumplir con la obligación de informar cuando se trata de una medida proporcionada y necesaria para los fines que se persiguen, los cuales son, en este caso, excepcionales.

Algo similar ocurre en la STC 39/2016[32], cuyo procedimiento se inicia por la instalación de una cámara de videovigilancia para controlar la caja registradora en la que trabajaba una trabajadora de INDITEX tras detectar irregularidades a través de un sistema de control informático de caja. Esta instalación se hizo sin comunicar a los trabajadores sobre ella, aunque existía un cartel informativo de videovigilancia.

6.3. Empleado VS Universidad de Sevilla

Sentencia del Tribunal Constitucional nº 29/2013[33].

Al igual que la anterior sentencia tratada en este epígrafe, este caso también acaba siendo condicionador de la decisión del TEDH por su trascendencia en nuestra jurisprudencia más reciente en relación con el uso de la videovigilancia.

Sin embargo, en esta ocasión el uso de sistemas de videovigilancia no se dirige hacia la apropiación de dinero por parte de trabajadores, sino hacia el control de la jornada laboral de los trabajadores.

Este procedimiento lo inicia un trabajador de la Universidad de Sevilla por la utilización de unas grabaciones supuestamente utilizadas de forma ilícita como prueba en las sanciones disciplinarias impuestas por la Universidad.

Para poner en antecedentes, relataremos brevemente los hechos que dieron lugar a este proceso.

La Universidad de Sevilla, para la que trabaja el recurrente de la sentencia, *"sospecha de irregularidades en el cumplimiento de su jornada laboral"*, por lo que decide

[32] Sentencia del Tribunal Constitucional (Pleno) nº 39/2016, de 3 de marzo. Ponente: Doña Encarnación Roca Trías. Roj: RTC 2016\39.

[33] Sentencia del Tribunal Constitucional (Sala Primera) nº 29/2013, de 11 de febrero. Ponente: Don Fernando Valdés Dal-Ré. Roj: RTC 2013\29.

comenzar a controlar la asistencia del recurrente a su puesto de trabajo. Para ello, la Universidad utiliza el sistema de videovigilancia ya instalado en los accesos a las dependencias durante 2 meses.

Por otra parte, la firma de asistencia del trabajador en cuestión se realiza todos los días a la hora en que se inicia su jornada laboral.

Gracias a las grabaciones captadas, se observan diferencias de entrada y salida con respecto a la firma realizada por el trabajador de cerca de una hora.

Ante esta irregularidad, la Universidad de Sevilla le impone tres sanciones de suspensión de empleo y sueldo por *"faltas reiteradas e injustificadas de puntualidad en la entrada al trabajo durante diez o más días en un mes, […] transgresión de la buena fe contractual y abuso de confianza, consistente en hacer constar en las hojas de control de asistencia una hora de entrada al trabajo que no se corresponde con la real, y faltas de asistencia injustificadas al trabajo durante más de tres días en un mes"*.

Es por esto por lo que el trabajador presenta la demanda, manifestando que las grabaciones obtenidas habían constituido de manera ilegal una prueba que dio lugar a las sanciones impuestas.

El recurrente, en su demanda de amparo, hace referencia y fundamenta sus alegaciones en la STC 292/2000[34], de tal forma que considera que su derecho fundamental a la protección de datos recogido en el apartado 4 del artículo 18 de la CE estaba siendo vulnerado *"con la utilización no consentida ni previamente informada de las grabaciones"* para controlar su jornada laboral, lo que daría lugar a la nulidad de éstas y, por tanto, de las sanciones impuestas por parte de la Universidad de Sevilla, pues estaban basadas en las grabaciones objeto de anulación.

Tal y como sustrae el Tribunal del apartado 4 del artículo 18 CE, el fin del derecho fundamental a la protección de datos es otorgar a su titular *"un poder de control sobre sus datos personales, sobre su uso y destino"*, pero, en este caso, al no informar al trabajador de qué fin iban a tener las imágenes captadas por las cámaras, no podría ejercer ese poder.

A diferencia de lo ocurrido en la STC 186/2000, en este caso estamos ante un fin distinto al que se informó a la hora de la instalación del sistema de videovigilancia. Además, en aquel caso, las cámaras se colocaron enfocando al puesto de trabajo, al

[34] Sentencia del Tribunal Constitucional (Pleno) nº 292/2000, de 17 de diciembre. Ponente: desconocido. Roj: JUR 2014\26887.

contrario que en el caso actual, en el que se utilizan cámaras de videovigilancia que se encuentran en *"vestíbulos y lugares públicos de paso"*.

Además, la fundamentación de la falta de información en el poder del empresario de controlar la actividad laboral no tendría cabida tampoco, pues esa omisión *"haría quebrar la efectividad del derecho fundamental, en su núcleo esencial"*. Es por ello que, en este caso, estaríamos ante un tratamiento de datos personales ilícito, pero que está viciado por un encubrimiento de la información que ha de estar en conocimiento del trabajador en cuestión.

Así pues, el Tribunal considera vulnerado el artículo 18.4 CE. A esta conclusión alega el tribunal, además, que de nada sirve el cartel informativo ubicado en las entradas de los edificios videovigilados por la Universidad de Sevilla, pues el fin que es tratado en este procedimiento es distinto a los establecidos e informados a los trabajadores en el momento en el que se instaló el sistema de videovigilancia que captó las imágenes objeto del litigio.

Finalmente, el Tribunal declara la nulidad de las grabaciones como prueba principal de las irregularidades en la jornada laboral y de las sanciones impuestas al trabajador por parte de la Universidad.

Visto el caso tratado por esta Sentencia del Tribunal Constitucional, podemos observar que, aunque la legislación vigente permita al empresario llevar a cabo un tratamiento de datos personales, éste no puede considerarse lícito si no ha sido informado a los trabajadores a los que afectará éste.

Por otro lado, se puede deducir de esta sentencia que la colocación de cámaras de videovigilancia en zonas de descanso y recreo para los trabajadores con el fin de controlar la asistencia a su puesto de trabajo o su efectividad laboral, pues se trata de una medida intrusiva en la intimidad de éstos. Esto nos lleva a decir que estamos, en este caso, ante una medida desproporcionada, debido a que existen medidas menos agresivas para alcanzar el mismo fin perseguido, tales como ubicar las cámaras, no en lugares de paso o recreo, sino en los puestos de trabajo.

7. CASOS COTIDIANOS DE LA VIDEOVIGILANCIA

Este epígrafe de nuestro trabajo, como veremos a continuación, versará sobre las situaciones más habituales de videovigilancia con las que nos podemos encontrar en nuestra vida cotidiana. Sin embargo, estas circunstancias o situaciones, si bien suelen

pasar desapercibidas por el ciudadano medio, tienen gran importancia a la hora de captar ciertos datos de personas ajenas a los tratamientos que se realicen de estos.

Es por ello que trataremos estas situaciones de una forma breve, pero a la vez contundente, con el fin de que se tenga presente en qué posición y lugar debe utilizarse a la hora de colocar las cámaras de videovigilancia.

7.1. Centros educativos de menores

Ésta será la primera situación o lugar a la que nos referiremos. Le otorgamos este primer lugar por la importancia de los datos que las cámaras de videovigilancia puedan captar, pues hay que tener presente que en los centros educativos como guarderías, ludotecas o colegios se van a realizar grabaciones en las que aparecerán menores de edad, en muchas ocasiones sin propio conocimiento de que son grabados.

Por tanto, debemos tener mucha precaución a la hora de instalar un sistema, evitando poner en riesgo, de esta manera, datos sensibles pertenecientes a niños.

Así pues, de acuerdo con la Guía sobre el uso de videocámaras para seguridad y otras finalidades[35] de la AEPD, la instalación de un sistema de videovigilancia en estos centros ha de ser *"proporcional en relación con la infracción que se pretenda evitar"*.

La guía antes mencionada enumera una serie de indicaciones que deben tenerse en cuenta a la hora de la instalación del sistema de videovigilancia, las cuales pasamos a comentar a continuación:

- **Debe grabarse el mínimo espacio posible para alcanzar el fin perseguido.** En este sentido, la guía limita el espacio grabado a los espacios públicos, tales como pasillos o accesos al centro.
- **No podrán grabarse lugares que estén protegidos por el derecho a la intimidad.** En esta ocasión, debemos entender por tales sitios los aseos y vestuarios, y aquellos en los que *"se desarrollen actividades cuya captación pueda afectar a la imagen o a la vida privada"*, como podría ser un gimnasio.
- **Se pueden instalar cámaras en patios de recreo y comedores.** No obstante, sólo se podrá cuando lo que se pretenda proteger el interés superior del menor, pues ha de tratarse de lugares en los que exista la posibilidad de que se produzcan acciones que pongan en riesgo su integridad física, psicológica y emocional.

[35] Guía sobre el uso de videocámaras para seguridad y otras finalidades, publicada por la AEPD. Enlace al documento: https://www.aepd.es/sites/default/files/2019-09/guia-videovigilancia.pdf

- **Se considera desproporcionada la grabación dentro de *"las aulas mientras los alumnos realizan pruebas de nivel de conocimientos".*** Lo que deja en el aire el resto del tiempo que los menores permanecen en el aula.
- **Las grabaciones obtenidas con el fin de controlar la asistencia escolar están prohibidas, salvo excepciones.**

De acuerdo con estas indicaciones, podemos deducir que, para garantizar la seguridad del centro, solo se permite la instalación de sistemas de videovigilancia en zonas de esparcimiento y recreo, como son los pasillos o el patio de recreo. Sin embargo, existen situaciones excepcionales en las que podremos instalar un sistema de videovigilancia en las aulas.

Una circunstancia excepcional que legitimaría la instalación de un sistema de videovigilancia en el interior de un aula sería aquella en la que el tutor de los alumnos es sospechoso de causar lesiones o vejaciones en los alumnos, de tal forma que la grabación pueda constituir una prueba de peso en el procedimiento iniciado para condenar a dicho profesor.

Otro lugar en el que queda limitado el uso de videocámaras es el comedor en el que los alumnos comen a menudo, pues éstas sólo podrán instalarse con el fin de proteger el interés superior del menor. De esta forma, podría sustituirse la presencia de adultos por una videovigilancia que permita controlar la convivencia de los alumnos entre ellos en un momento en el que no hay o es escasa la presencia de monitores que puedan solucionar conflictos o accidentes que se ocasionen en ese lugar.

Por último, debemos hacer referencia a la utilización de la videovigilancia para controlar la asistencia de los menores al centro educativo objeto de grabación, tal y como establece la guía sobre el uso de videocámaras para seguridad y otras finalidades de la AEPD en sus indicaciones. La prohibición de este uso de la videovigilancia se debe a la desproporcionalidad de la medida, pues se trata de un fin que puede ser alcanzado a través de otros tipos de medidas, tales como una lista de asistencia rellenada a mano o telemáticamente por el monitor de los alumnos.

7.2. Comunidades de propietarios

7.2.1. Zonas comunes

Un caso muy distinto al anterior es el de las comunidades de propietarios. En esta ocasión se captarán imágenes de zonas comunes de comunidades de propietarios o vecinos.

Para ello será necesario el acuerdo de la junta de propietarios de acuerdo con el artículo 17, apartado 3, de la Ley 49/1960[36], de 21 de julio, *sobre propiedad horizontal*, el cual establece que *"el establecimiento o supresión de los servicios de portería, conserjería, vigilancia u otros servicios comunes de interés general […] requerirán el voto favorable de las tres quintas partes del total de los propietarios que, a su vez, representen las tres quintas partes de las cuotas de participación".*

Las cámaras instaladas en estas zonas sólo deben captar las zonas comunes de la comunidad en cuestión. En este sentido, debemos entender por zonas comunes los pasillos, descansos y entrada del edificio de viviendas. Junto a estos lugares, debemos incluir instalaciones deportivas, piscina, jardines y garajes abiertos con los que cuente la vecindad.

No obstante, esta grabación interior y privada no exime del cumplimiento de información mediante un cartel identificativo, al igual que los demás casos que ya hemos analizado a lo largo de este trabajo.

Finalmente, tal y como establece la Guía sobre el uso de videocámaras para seguridad y otras finalidades de la AEPD, *"el acceso a las imágenes estará restringido a las personas designadas por la comunidad de propietarios"*.

7.2.2. Plazas de garaje

No es inusual encontrarse en la situación de que la comunidad en la que residimos no considera oportuno llevar a cabo la instalación de un sistema de videovigilancia, pero, en cambio, nosotros consideramos útil dicha instalación para proteger nuestra vivienda y, en especial, nuestro vehículo, el cual se encuentra en un garaje abierto en el que cualquier vecino o persona con acceso al recinto puede dañar nuestro patrimonio.

Es por ello que la AEPD ha considerado conveniente recoger esta situación en su guía sobre el uso de la videovigilancia.

Para la instalación de estas cámaras es necesario que sólo se capte la imagen de la plaza de garaje objeto de la videovigilancia, permitiéndose un margen de extralimitación del espacio grabado, el cual será inevitable captar por parte de la videocámara. Además, al igual que en la anterior situación, será necesaria la autorización de la Junta de Propietarios para que se lleve a cabo dicha instalación.

[36] Ley 49/1960, de 21 de julio, sobre propiedad horizontal. Enlace al documento: https://www.boe.es/buscar/act.php?id=BOE-A-1960-10906

El Informe Jurídico de la AEPD 2014/0003[37] aborda este tema basándose en una consulta acerca de la instalación de una cámara de videovigilancia por parte de un propietario en el garaje propiedad de la comunidad de propietarios.

En esta ocasión, el propietario instala una videocámara que capta imágenes de varias plazas de garaje que no corresponden a éste, lo que lleva a la AEPD a dictaminar que *"no se cumplen los requisitos señalados que vendrían a legitimar el tratamiento de los datos por el consultante"*, puesto que se está afectando al derecho a la intimidad de las personas que hacen uso de esas plazas que no corresponden al consultante.

7.3. Parkings públicos y matrículas

Este es un caso muy común y apenas apreciado. Esto se debe a que nos encontramos ante un dato muy curioso, el cual no es nuestro nombre, teléfono o dirección, sino la matrícula de nuestro vehículo.

Debemos tener en cuenta que esa numeración, que identifica a nuestro vehículo, es lo que hace que nuestro vehículo sea distinto del resto.

Tal y como ya reflejó la AEPD en el Informe Jurídico 425/2006[38], *"el tratamiento de los datos correspondientes a las placas de matrícula de los vehículos se encontrará sometido a lo dispuesto en la"* LOPD-GDD. Esto se debe a lo que, en su momento, establecía el artículo 3.a) de la LOPD.

Así pues, de acuerdo con la entonces vigente Directiva 95/46/CE[39] del Parlamento y del Consejo, de 24 de octubre de 1995, *relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos profesionales y a la libre circulación de estos datos,* una persona será identificada o identificable cuando su identidad *"pueda determinarse, directa o indirectamente, en particular mediante un número de identificación"*.

A esta definición, la AEPD establece un límite para la interpretación del concepto identificable. De esta manera, la AEPD establece que ha de considerarse como

[37] Informe jurídico nº 2014/0003 de la AEPD sobre la instalación de videocámaras en un garaje comunitario. Enlace al documento: https://www.aepd.es/es/documento/2014-0003.pdf

[38] Informe Jurídico nº 425/2006 de la AEPD sobre el tratamiento de la matrícula como dato personal o no. Dicho informe ha sido eliminado del sitio web de la AEPD, aunque a día de hoy queda constancia de él en distintos blogs, artículos de periódico y demás lugares online. Enlace al documento: http://www.delere.es/ficheros/Informe%20AEPD%20Matr%C3%ADcula%20como%20dato%20de%20car%C3%A1cter%20personal.pdf. Esta decisión fue reiterada posteriormente en varias ocasiones, como puede ser el del Informe Jurídico de la AEPD nº 297/2012 (enlace al documento: https://www.aepd.es/es/documento/2012-0297.pdf).

[39] Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos profesionales y a la libre circulación de estos datos. Enlace al documento: https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

identificable a aquella persona cuya identificación *"no requiere plazos o actividades desproporcionados"*. A esta reducción de plazos para identificar a una persona ayudaría la publicidad del Registro de Vehículos que reconocía el Reglamento General de Vehículos aprobado por el Real Decreto 2822/1998[40].

La Audiencia Nacional, en la sentencia de 26 de diciembre de 2013[41], por la que una comunidad de vecinos pretende impugnar la sanción impuesta a ésta por la AEPD mediante la resolución de 2 de diciembre de 2011, considera que las imágenes captadas por las cámaras de videovigilancia son datos de carácter personal. Sin embargo, *"ello ha de entenderse referido a imágenes de personas, y no a imágenes de placas o números de matrícula cuya caracterización como dato de carácter personal"*, pues, como bien dijimos al inicio de este subapartado, esta numeración diferencia a nuestro vehículo del resto, por lo que se trata de un dato que identifica a un vehículo, no a una persona, *"ya que el conductor del vehículo ni siquiera tiene porqué ser el titular del mismo"*.

De esta manera, la jurisprudencia existente ha consolidado la postura que defiende que la matrícula de nuestro vehículo no es un dato personal.

Por esto, la videovigilancia de los parkings públicos, si bien trata las imágenes como datos, éstas sólo son referentes a las personas que en ellas aparecen, no a las matrículas de los vehículos.

8. LOS CUERPOS Y FUERZAS DE SEGURIDAD DEL ESTADO EN LA VIDEOVIGILANCIA

Este epígrafe va dirigido a poner en relieve el papel de las Fuerzas y Cuerpos de Seguridad del Estado en la utilización de cámaras de videovigilancia en la vía pública.

Como ya comentamos anteriormente, la grabación de las zonas públicas desde el espacio privado está muy limitada en nuestro país, quedando muy ligada a los Cuerpos y Fuerzas de Seguridad del Estado.

En este segmento de la videovigilancia, ésta quedará regulada principalmente por la Ley Orgánica 4/1997[42].

[40] Real Decreto 2822/1998, de 23 de diciembre, por el que se aprueba el Reglamento General de Vehículos. Enlace al documento: https://www.boe.es/buscar/doc.php?id=BOE-A-1999-1826

[41] Sentencia de la Audiencia Nacional de 26 diciembre 2013. Ponente: Doña Nieves Buisán García. Roj: JUR 2014/27818.

[42] Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. Enlace al documento: https://www.boe.es/buscar/doc.php?id=BOE-A-1997-17574

Con esta norma se pretende regular la utilización de estos instrumentos para *"contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos"*. De esta manera, se busca tener un control absoluto de las imágenes captadas de personas sin su consentimiento, persiguiendo siempre un interés público general, lo que legitima el tratamiento de estos datos a tenor del apartado 1.e) del artículo 6 del RGPD.

En primer lugar, hay que tener presente que existe una importante dificultad para obtener el consentimiento expreso del interesado en la vía pública, lo que haría muy difícil el tratamiento de las imágenes captadas por las cámaras de videovigilancia.

Esto es lo que ocurre con El Corte Inglés en la SAN nº 659/2011[43], por la que se recurre la resolución de la AEPD por la utilización de videovigilancia exterior en sus edificios de Málaga.

El Corte Inglés está conformado en este municipio por dos edificios, los cuales se encuentran vigilados por un sistema de 8 videocámaras, las cuales tienen un ángulo de 360º y cuentan con una función de zoom.

Tal y como declara la Audiencia Nacional en esta sentencia, *"la grabación en lugares públicos debe realizarse por las Fuerzas y Cuerpos de Seguridad del Estado"*, hecho que aquí realiza una empresa privada de seguridad después de haber solicitado a la Secretaría de Estado de Interior la concesión de la autorización pertinente de la instalación del sistema de videovigilancia exterior y de haber recibido la negativa contestación por parte de este organismo.

Todo esto hace que sea el Estado quien convierta estas grabaciones en un tratamiento que busca un interés público general, ya sea éste la reducción de actos delictivos o mejorar la seguridad vial del tráfico.

De acuerdo con el artículo 3 de la LO 4/1997, la instalación de videocámaras por parte de las Fuerzas y Cuerpos de Seguridad del Estado ha de cumplir una serie de requisitos que trataremos más adelante, pero, además, requiere de una autorización del Delegado del Gobierno en la Comunidad Autónoma y un informe previo de *"un órgano colegiado presidido por un Magistrado y en cuya composición no serán mayoría los miembros dependientes de la Administración autorizante"*. Dicha autorización tendrá una vigencia anual, pudiéndose renovar a su término.

[43] Sentencia de la Audiencia Nacional nº 659/2011, de 10 de febrero de 2011. Ponente: José Guerrero Zaplana. Roj: SAN 659/2011.

La ley diferencia entre dos tipos de cámaras que podrán ser objeto de utilización por parte de los Cuerpos y Fuerzas de Seguridad del Estado, de tal forma que podremos diferenciar entre instalaciones fijas y videocámaras móviles.

En la autorización de la instalación de cámaras fijas, de acuerdo con el artículo cuarto de la ley antes citada, se tendrá en cuenta el fin para el que se van a fijar éstas. Entre los posibles fines, destacan la protección de edificios públicos y de instalaciones destinadas a la defensa de España y prevenir actos delictivos.

En lo que respecta a las videocámaras móviles, su uso deberá contar con la autorización del *"máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad"*, según lo establecido en el artículo 5 de la Ley Orgánica 4/1997. Estas cámaras pueden ubicarse junto a otras fijas o en otros lugares públicos, y habrá que informar de su uso cada quince días a la Comisión que recoge el artículo 3.

De acuerdo con el artículo 6 de la Ley Orgánica 4/1997, de 4 de agosto, *por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos*, las cámaras de videovigilancia han de ser utilizadas con proporcionalidad, persiguiendo la idoneidad y el principio de intervención mínima.

Atendiendo a estos principios de utilización, las videocámaras sólo pueden utilizarse para el *"mantenimiento de la seguridad ciudadana"*. Además, habrá que tener en cuenta, en lo que se refiere al principio de intervención mínima, la finalidad que se busca con su utilización y la posible intrusión en el derecho al honor, a la propia imagen y a la intimidad de las personas que van a ser objeto de las grabaciones.

En resumen, observamos que, salvo autorización expresa, la grabación de espacios públicos a través de un sistema de videovigilancia, fijo o móvil, queda supeditada a las Fuerzas y Cuerpos de Seguridad del Estado. Éstas, buscarán mantener la seguridad de las personas y los bienes, consiguiendo así una mejor convivencia.

9. NUEVAS TECNOLOGÍAS EN LA VIDEOVIGILANCIA

Vivimos en un mundo en el que la tecnología avanza a pasos agigantados, caracterizándose ésta por una complejidad y movilidad cada vez mayor. Esto ha conseguido que podamos capturar imágenes con un teléfono móvil o una minicámara.

Es por la facilidad de grabar nuestro alrededor por lo que no podemos dejar de lado a la tecnología emergente en nuestro trabajo. Para ello, en este epígrafe trataremos rápidamente la captación de imágenes por drones y por las cada vez más utilizadas "cámaras on board" o "cámaras a bordo".

9.1. Cámaras a bordo o cámaras "on board"

Este tipo de cámaras se instala en el interior del vehículo o en el casco del piloto, dependiendo del tipo de vehículo al que nos estemos refiriendo. Con ellas se pretende grabar el trayecto realizado por el vehículo en el que son instaladas y servir como prueba visual en caso de que se produjese algún incidente.

De esta manera, cuando las grabaciones realizadas sólo pretenden grabar el trayecto para disfrute propio del propietario o conductor del vehículo, no deberá aplicarse la legislación aplicable de protección de datos, tal y como establece el artículo 2 RGPD en su apartado 2.c).

No obstante, cuando las imágenes son captadas para obtener pruebas de un posible accidente de tráfico, éstas quedarán sometidas a la LOPD-GDD por su tratamiento, que quedará legitimado por el artículo 6.1.f), es decir, que dicho tratamiento *"es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero"*. Como declara la Guía sobre el Uso de Videocámaras para Seguridad y Otras Finalidades de la Agencia Española de Protección de Datos, esta legitimación vendría a proteger el derecho del afectado a una tutela judicial efectiva, el cual es un derecho fundamental que reconoce la Constitución Española de 1978.

9.2. Drones

En este subapartado vamos a tratar la videovigilancia desde el punto de vista aéreo a través de los recientes drones, los cuales están causando graves problemas en algunas zonas por su peligrosidad o por la captación de imágenes comprometidas. Ello se debe a la falta de regulación existente en un ámbito tan novedoso como éste.

Para comenzar, realizaremos una breve explicación de qué es un dron y para qué sirve.

De acuerdo con la descripción que nos ofrece la Real Academia de la Lengua Española, un dron es una aeronave no tripulada.

Para ahondar un poco más en este elemento, podemos decir que se trata de un aparato teledirigido que puede constar de distintos tipos de sensores y herramientas a través de las cuales se pueden procesar y tratar muy diversos datos, tales como las imágenes. Por ello trataremos aquí este tipo de productos.

Tal y como ofrece la Guía de Drones y Protección de Datos[44] de la AEPD, sólo una serie de operaciones quedan sometidas a la legislación de Protección de Datos, aunque

[44] Guía de Drones y Protección de Datos, publicada por la AEPD. Enlace al documento: https://www.aepd.es/sites/default/files/2019-09/guia-drones.pdf

existen otras que, dependiendo de las circunstancias en las que se realicen las grabaciones, pueden quedar sometidas o no a protección de datos. Entre estas operaciones se pueden destacar *"la inspección de infraestructuras, levantamientos topográficos, inspecciones y/o tratamientos en agricultura",* etc.

Además, estos tratamientos deben seguir una serie de directrices para que el uso de estas aeronaves sea correcto. La Guía antes mencionada enumera estas directrices o recomendaciones.

Una de las recomendaciones es que se disminuya la visualización de *"personas y objetos que permitan su identificación"* en el lugar donde se realice la grabación. De esta manera, se recomienda sobrevolar los espacios en los que se pretenda captar imágenes en los espacios horarios en los que haya menos afluencia de gente.

Junto a esto, se recomienda capturar las imágenes estrictamente necesarias, de tal forma que se capten los datos personales mínimos, con lo que se estaría cumpliendo el artículo 5.1.c) del RGPD, por el que se utilizarán los datos personales *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"*.

En el caso de que se trate de lugares en los que siempre hay personas, las imágenes han de ser capturadas lo suficientemente lejos como para que aquellas no puedan ser identificadas.

Como se puede observar, estas recomendaciones buscan que los tratamientos que vayan a realizarse cumplan con los principios establecidos por el RGPD en su artículo 5.

En lo que respecta al tratamiento de datos personales a través de la captación de imágenes desde un dron, hay que atenerse a lo establecido en la LOPD-GDD. No obstante, este tratamiento podría quedar sometido a la LO 4/1997, de tal manera que el uso de los drones para el tratamiento de datos personales se restringiría a los Cuerpos y Fuerzas de Seguridad del Estado y a las autorizaciones que estos diesen de acuerdo con dicha normativa al tratarse del uso de cámaras móviles de videovigilancia en espacio público.

Para este tipo de uso de los drones, la Guía de Drones y Protección de Datos ofrece también una serie de consideraciones a tener en cuenta, como es la de *"elegir la tecnología a bordo más adecuada a la finalidad que se persigue"*, tomar todas las medidas necesarias para proteger los datos procesados y los mecanismos requeridos para informar del tratamiento, como es el establecimiento de carteles informativos, *"eliminar o anonimizar cualquier dato personal innecesario"*, o incrementar la visualización de los drones, haciéndolos identificables y permitiendo al interesado no entrar en el campo de

captación de dicha cámara, lo cual puede realizarse con la utilización de colores llamativos que contrasten con el área en el que se encuentra el dispositivo.

Junto a esto, hay que tener en cuenta que el dron que se vaya a utilizar para el tratamiento de datos ha de cumplir con la legislación aplicable a las aeronaves no tripuladas para que puedan surcar el cielo desde el que realizarán su función para obtener los datos personales. Para ello, debemos dirigirnos al Real Decreto 1036/2017[45], de 15 de diciembre, *por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea*.

10. CONCLUSIONES

Una vez analizadas las limitaciones a las que se encuentra sometida la videovigilancia en nuestro país, tanto por legislación interna como europea, así como por la jurisprudencia asentada por los Tribunales, podemos llegar a una serie de conclusiones.

En primer lugar, hemos podido observar que, al ser un ámbito tan amplio, nuestro poder legislativo ha tenido que limitar su uso mediante la elaboración de una compleja legislación que, aunque bien organizada, puede llevar a conflictos o confusiones en el usuario de un sistema de cámaras de seguridad.

En segundo lugar, debemos hacer referencia a la armonización de la legislación de protección de datos en los Estados miembros de la Unión Europea. Esta acción ha conseguido un nuevo acercamiento entre los países europeos, que han tenido que basar su legislación interna en la dictada por la Unión Europea. Tal es el caso de nuestro país con la derogación de la anterior LOPD (LO 15/1999) por la nueva LOPD-GDD (LO 3/2018).

En tercer lugar, como se ha podido analizar, la limitación en el ámbito laboral es muy restrictiva, pero proviene principalmente de la jurisprudencia existente en nuestro país, no de la legislación vigente en cada momento. En este sentido, el legislador ha otorgado un gran poder de control al empresario sobre sus trabajadores, que ha sido

[45] Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea. Enlace al documento: https://www.boe.es/buscar/doc.php?id=BOE-A-2017-15721

corroborado por los tribunales en los distintos casos que han suscitado controversias en relación con su derecho a la intimidad.

En último lugar, como muestra del avance de nuestra sociedad, no podemos dejar de lado el crecimiento de las nuevas tecnologías, que se han ido incorporando a la videovigilancia gracias a la instalación o integración de elementos de captación de imágenes a aparatos tecnológicos que siguen mejorando con el paso del tiempo y podrían mejorar nuestra seguridad y la de nuestros patrimonios de una manera más eficaz. No obstante, estas nuevas tecnologías también afectarán nuestra intimidad, por lo que habrá que regular su uso para evitar estos daños, hecho este que ya se está realizando desde hace poco tiempo.

11. ABREVIATURAS

RGPD	REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
AEPD	Agencia Española de Protección de Datos.
CE	Constitución Española (de 1978).
LO 1/1982	Ley Orgánica, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
LOPD-GDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
LET	Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
TEDH	Tribunal Europeo de Derechos Humanos

12. BIBLIOGRAFÍA

- Gil Membrado, Cristina (2019), *Videovigilancia y protección de datos: Especial referencia a la grabación de la vía pública desde el espacio privado,* Wolters Kluwer España, S.A..
- Mella Méndez, Lourdes y otros (2017), *Nuevas tecnologías y nuevas maneras de trabajar: Estudios desde el Derecho Español y comparado,* "Capítulo IX: El control empresarial a través de medios de videovigilancia", Madrid, Dykinson, páginas 215-228.
- Cobos Tubilla, Jesús y otros (2018), *Protección de datos: Aplicación del RGPD,* Madrid, Francis Lefebvre.
- Hernández Fernández, Abelardo (2009), *El honor, la intimidad y la imagen como derechos fundamentales: [Su protección civil en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo]*, Madrid, Colex.

13. LEGISLACIÓN

- Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente.
- Carta de los Derechos Fundamentales de la Unión Europea, aprobada en Niza el 7 de diciembre y de 2000.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos profesionales y a la libre circulación de estos datos. *(derogada)*
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *(derogada)*
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil de derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Ley 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
- Ley 49/1960, de 21 de julio, sobre propiedad horizontal.
- Real Decreto 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- Real Decreto 2822/1998, de 23 de diciembre, por el que se aprueba el Reglamento General de Vehículos.
- Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea.

- Real Decreto Legislativo 2/1995, de 7 de abril, por el que se aprueba el texto refundido de la Ley de Procedimiento Laboral.
- Guía sobre el uso de videocámaras para seguridad y otras finalidades, publicada por la AEPD.
- Guía para el cumplimiento del deber de informar, publicada por la AEPD.
- Guía de Drones y Protección de Datos, publicada por la AEPD.

14. JURISPRUDENCIA

- Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) nº 144/2019, de 17 de octubre. Caso López Ribalda y otros contra España.
- Sentencia del Tribunal Europeo de Derechos Humanos nº 2018\1, de 9 de enero. Caso López Ribalda y otros contra España.
- Sentencia del Tribunal Constitucional (Pleno) nº39/2016, de 3 de marzo.
- Sentencia del Tribunal Constitucional (Pleno) nº 292/2000, de 17 de diciembre.
- Sentencia del Tribunal Constitucional (Sala Primera) nº 29/2013, de 11 de febrero.
- Sentencia del Tribunal Constitucional (Sala Primera), de 10 de julio.
- Sentencia del Tribunal Constitucional (Sala Primera) nº 110/1984, de 26 de noviembre.
- Sentencia del Tribunal Constitucional (Sala Primera) nº 124/1999, de 28 de junio.
- Sentencia del Tribunal Constitucional (Sala Primera) nº 98/2000, de 10 de abril.
- Sentencia del Tribunal Constitucional nº 57/1994, de 28 de febrero.
- Sentencia de la Audiencia Nacional nº659/2011, de 10 de febrero de 2011.
- Sentencia del Tribunal Superior de Justicia de Andalucía, Málaga (Sala de lo Social, Sección 1ª) nº 1268/2017, de 5 de julio.
- Instrucción 1/2006, de 8 de noviembre de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.