En este sentido:

a) La **base jurídica** del tratamiento de datos puede ser el **contrato de trabajo**, en relación con el art. 20.3 del ET, cuando la finalidad consiste en el control de las personas trabajadoras, pero también podría ser el **interés legítimo** del empleador, si el propósito fuera distinto, por ejemplo, la protección de los bienes empresariales.

Ejemplo.
Un empresario dispone de una sala de servidores en la que se almacenan en formato digital datos sensibles de la empresa, datos personales de las personas trabajadoras y datos personales de los clientes. Para cumplir las obligaciones legales de proteger los datos contra el acceso no autorizado, el empresario ha instalado un sistema de control de acceso que registra la entrada y salida de las personas trabajadoras que tienen permiso para entrar en la sala. Si desaparecen elementos del equipo o algún dato es objeto de acceso no autorizado, pérdida o robo, los registros guardados por el empresario le permiten determinar quién tuvo acceso a la sala en ese momento. Habida cuenta de que el tratamiento es necesario y no vulnera el derecho a la vida privada de las personas trabajadoras, este puede ser en el interés legítimo si las personas trabajadoras han sido informadas adecuadamente sobre la operación de tratamiento. Sin embargo, la observación continua de la frecuencia y los tiempos exactos de entrada y salida de las personas trabajadoras no puede justificarse si estos datos se utilizan también para otros fines, como la evaluación del desempeño (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29).

b) Deben evitarse sistemas de acceso **especialmente invasivos** de los derechos fundamentales de las personas trabajadoras si existen otros igualmente eficaces que resulten menos intrusivos.

c) En caso de utilización de **datos biométricos, véase** capítulo 4.6.

3. VIDEOVIGILANCIA

La imagen es un dato personal, ya que identifica o hace identificable a una persona. En este sentido, la instalación de cámaras, con finalidades como la seguridad, el control laboral, el acceso a zonas restringidas captando la matrícula del coche y la imagen del conductor, o incluso la monitorización de una UVI, supondría un tratamiento de datos de carácter personal y, en consecuencia, resultaría de aplicación la normativa de protección de datos.

El tratamiento de datos con fines de videovigilancia se regula en el art. 22 de la LOPDGDD. Según el art. 89 de la LOPDGDD, estas imágenes pueden tratarse para el ejercicio de las funciones de control de las personas trabajadoras, con los siguientes requisitos:

1. La **base jurídica** para el control de las personas trabajadoras mediante videovigilancia es el contrato de trabajo y las facultades legales de control concedidas al empleador (art. 20.3 del ET), por lo que no se requiere el consentimiento.

2. La videovigilancia sólo debe utilizarse cuando no sea posible acudir a otros medios que causen **menos impacto** en la privacidad. En este sentido, los sistemas de videovigilancia para control empresarial sólo se adoptarán cuando exista una relación de **proporcionalidad** entre la finalidad perseguida y el modo en que se traten las imágenes y no haya otra

medida más idónea. El control audiovisual ha de respetar los derechos fundamentales de la persona trabajadora, especialmente el derecho a la intimidad personal (STC 98/2000, de 10 abril y 186/2000, de 10 julio).

Ejemplo.
La tecnología permitiría que a través de la videovigilancia un empresario observe las expresiones faciales de trabajador por medios automatizados, identifique desviaciones con respecto a los patrones de movimiento predefinidos, etc. Esto sería desproporcionado a efectos de los derechos y libertades de los trabajadores y, por tanto, ilícito. El tratamiento también puede implicar la elaboración de perfiles y, posiblemente, la toma de decisiones automatizadas. Por tanto, la videovigilancia no puede utilizarse en combinación con otras tecnologías, como el reconocimiento facial, porque en tal caso el control resulta desproporcionado (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29).

3. El **principio de minimización** del art. 5 del RGPD requiere que los datos personales tratados sean adecuados, pertinentes y limitados en relación con los fines para los que son tratados.

En el ámbito de la videovigilancia este principio supone:

a) Que el **número de cámaras** se limite a las necesarias para cumplir la función de vigilancia.

b) Que el responsable analice también los **requisitos técnicos** de las cámaras, ya que el zoom, o las denominadas "cámaras domo" pueden afectar al citado principio de minimización.

Asimismo, los **monitores de grabación** deben situarse de forma que, en la medida de lo posible, únicamente puedan ser visualizados por aquellos cuya función sea controlar los equipos que realizan las grabaciones. En ningún caso deben estar ubicados de forma que clientes o usuarios puedan ver las imágenes.

4. La empresa debe **informar** a las personas trabajadoras y, en su caso, a sus representantes, con carácter previo, y de forma expresa, clara y concisa, acerca de esta medida.

5. En el supuesto de que se haya captado la **comisión flagrante de un acto ilícito** por las personas trabajadoras, se entenderá cumplido el deber de informar cuando se haya colocado un **dispositivo informativo** en lugar suficientemente visible concretando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos.

No obstante, la sentencia del Tribunal Europeo de los Derechos Humanos (STEDH López Ribalda II de 17-10-2019) admite, dadas las circunstancias del caso, que la no advertencia a la persona trabajadora, de forma concreta, sobre el emplazamiento de la cámara, en un supuesto en el que sí ha existido información sobre la instalación de cámaras de videovigilancia y concurre una sospecha fehaciente de incumplimiento grave de las obligaciones laborales (sustracción de productos de la empresa de forma continuada con alto valor económico) no conduce a la nulidad de las pruebas obtenidas para imponer una sanción a la persona trabajadora, pero la empresa puede ser considerada responsable en el ámbito de la protección de datos, por infracción de la obligación de informar, debiendo hacer frente a las responsabilidades civiles y administrativas que se puedan derivar de ese incumplimiento.

6. Se produce un tratamiento de datos tanto si las cámaras graban imágenes como si las reproducen en **tiempo real**. En cambio, no se aplica la normativa de protección de datos a las **cámaras simuladas**, pues, al no captar imágenes de personas físicas identificadas o identificables,

no tiene lugar un tratamiento de datos personales. En cambio, deberán aplicarse los principios vigentes en materia de protección de datos personales y la normativa sectorial que resulte de aplicación a las cámaras que simplemente estén **desactivadas** y que pueden ser activadas sin esfuerzos excesivos.

7. Está prohibida la instalación de sistemas de grabación de imagen y/o sonido en **lugares destinados al descanso o esparcimiento** de las personas trabajadoras, tales como vestuarios, aseos, comedores y análogos.

8. Deben implementarse las **medidas de seguridad** pertinentes, en función de los análisis de riesgos y, eventualmente, de la evaluación de impacto si fuera necesaria.

Cuando se trate de tratamientos de videovigilancia que entrañen un escaso riesgo, como podría ocurrir en comunidades de propietarios o pequeños establecimientos, puede utilizarse la herramienta de la AEPD denominada Facilita RGPD.

9. Si se encarga a un tercero la gestión de las cámaras, ese tercero se convierte en un **encargado del tratamiento**.

10. Respecto de la **supresión de los datos**, el art. 22.3 de la LOPDGDD permite su conservación durante un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

Finalmente, el art. 89 de la LOPDGDD limita la utilización de sistemas de grabación de sonidos en el lugar de trabajo, que se admitirá únicamente cuando se acrediten riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando los principios de proporcionalidad y de intervención mínima, así como las garantías indicadas para la videovigilancia.

4. GEOLOCALIZACIÓN

El art. 90 de la LOPDGDD permite el uso de sistemas de geolocalización para el **control de las personas trabajadoras**, aunque conviene tener en cuenta lo siguiente:

1. La **base jurídica** del tratamiento de datos no es el consentimiento, sino el contrato de trabajo y las facultades de control de **las personas trabajadoras** atribuidas legalmente a los empleadores.

2. Las **personas trabajadoras** y, en su caso, sus representantes deben ser **informados** de forma expresa, clara e inequívoca acerca de la existencia y características de estos dispositivos.

3. Las **personas trabajadoras** también deberán ser informadas acerca del posible ejercicio de los **derechos de acceso, rectificación, limitación del tratamiento y supresión**.

4. Los **principios de minimización y limitación de la finalidad** son plenamente operativos. Por consiguiente, si la finalidad de la geolocalización es el registro horario, los datos no podrán ser utilizados para verificar la ubicación de la persona trabajadora en cada momento, sino las horas de inicio y fin de la actividad, que es lo que permite la base jurídica del registro horario (art. 34.9 del ET).

5. El **principio de proporcionalidad** exige limitar esta clase de sistemas a aquellas situaciones donde no existan medios menos invasivos.