

Universidad Miguel Hernández de Elche
Facultad de Ciencias Sociales y Jurídicas de Elche
Titulación de Seguridad Pública y Privada
Trabajo Fin de Grado
Curso Académico 2025-2026



**Equilibrio entre seguridad y derecho a la
intimidad: análisis jurídico de la
videovigilancia en espacios laborales y
establecimientos abiertos al público**

Alumno: Víctor Manuel Botella Navarro

Tutora: Rosario Tur Ausina

INDICE

Resumen	4
Abstract	5
1. Introducción	6
1.1 Justificación	8
1.2 Objetivos	8
1.3 Metodología	9
2. Marco teórico	10
2.1. El derecho fundamental a la privacidad	10
2.1.1. Concepto de privacidad y distinción frente a intimidad	10
2.1.2. Evolución histórica del derecho a la privacidad	12
2.1.3. Tratamiento constitucional en el artículo 18 de la CE	12
2.1.4. La protección de datos como derecho fundamental autónomo	13
2.1.5. La perspectiva europea: de la Directiva 95/46/CE al RGPD	14
2.1.6. Privacidad, dignidad y autonomía personal	14
2.2. La seguridad y el control en las relaciones laborales y en los establecimientos abiertos al público	15
2.2.1. La seguridad como bien jurídico y función del Estado	15
2.2.2. Seguridad privada, control empresarial y prevención de ilícitos	15
2.2.3. El poder de dirección y control del empresario (art. 20.3 ET)	17
2.2.4. La prevención de pérdidas y riesgos en comercios y espacios de acceso público	18
2.2.5. Límites constitucionales y legales al control mediante videovigilancia	19
2.3. La videovigilancia laboral y en establecimientos abiertos al público	20
2.3.1. Concepto y tipologías: videovigilancia laboral, comercial y en comunidades de propietarios	20
2.3.2. Finalidades legítimas: control laboral, seguridad, prevención de delitos y protección del patrimonio	21
2.3.3. Videovigilancia manifiesta y encubierta	23
2.3.4. Impacto social y riesgos específicos para la privacidad de trabajadores y clientes	24
2.4. Límites jurídicos de la videovigilancia en el ámbito laboral y comercial	29
2.4.1. Principios del tratamiento de datos aplicables	29
2.4.2. Deberes del responsable del tratamiento	30
2.4.3. Obligaciones específicas del empresario y del titular del establecimiento	31

2.4.4. Derechos de los trabajadores y de los usuarios: información, acceso, oposición y tutela	32
2.4.5. Espacios especialmente protegidos: vestuarios, aseos, zonas de descanso	32
2.4.6. La grabación sonora, la videovigilancia encubierta y el uso de tecnologías avanzadas	32
2.5. Análisis jurisprudencial y doctrinal	34
2.5.1. Jurisprudencia del Tribunal Constitucional en materia de videovigilancia laboral	35
2.5.2. Doctrina del Tribunal Supremo	36
2.5.3. Jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) (<i>especial referencia al caso López Ribalda y otros contra España 2019</i>)	36
2.5.4. Resoluciones relevantes de la Agencia Española de Protección de Datos	37
2.5.5. Casos prácticos: centros de trabajo, comercios y comunidades de propietarios	37
2.5.6. Convergencias y divergencias en la doctrina de los tribunales	38
3. Propuesta de modelo de videovigilancia respetuoso con la privacidad en el ámbito laboral y comercial	39
4. Resultados	44
5. Conclusiones	48
A) NORMATIVA, DOCUMENTACIÓN Y JURISPRUDENCIA	52
B) REFERENCIAS BIBLIOGRÁFICAS	54

Resumen

El presente trabajo analiza el equilibrio entre las exigencias de seguridad y el derecho fundamental a la intimidad en el uso de sistemas de videovigilancia en el ámbito laboral y en los establecimientos abiertos al público. Para ello, se estudia la evolución normativa y jurisprudencial tanto en el ámbito nacional como europeo, prestando especial atención al principio de proporcionalidad como criterio esencial para valorar la legitimidad de estas medidas de control.

El estudio refleja que el ordenamiento jurídico dispone de mecanismos suficientes para proteger la privacidad frente a la videovigilancia. No obstante, también evidencia la existencia de conflictos prácticos derivados de la evolución tecnológica, del uso de grabaciones con fines disciplinarios en el ámbito laboral y de la incorporación progresiva de sistemas automatizados de análisis y control.

Finalmente, el trabajo desarrolla una propuesta de modelo de videovigilancia respetuoso con la privacidad, basada en la evaluación previa de proporcionalidad, la delimitación de finalidades, la minimización técnica, la transparencia y la responsabilidad proactiva. El objetivo no es cuestionar la legitimidad de las medidas de seguridad, sino garantizar que su aplicación resulte compatible con la protección de los derechos fundamentales en el marco de un Estado social y democrático de derecho.

Palabras clave: Videovigilancia; privacidad; intimidad; protección de datos; seguridad; derechos fundamentales; ámbito laboral.

Abstract

This paper analyses the balance between security requirements and the fundamental right to privacy in the use of video surveillance systems in the workplace and in establishments open to the public. To this end, it examines the legal and jurisprudential evolution of the subject at both national and European level, paying particular attention to the principle of proportionality as an essential criterion for assessing the legitimacy of these control measures.

The study shows that the legal system provides sufficient mechanisms to protect privacy in relation to video surveillance. However, it also highlights the existence of practical conflicts arising from technological developments, the use of recordings for disciplinary purposes in the workplace, and the progressive incorporation of automated systems for analysis and control.

Finally, the paper develops a proposal for a privacy-respectful video surveillance model based on prior proportionality assessment, limitation of purposes, technical minimisation, transparency, and proactive accountability. The aim is not to question the legitimacy of security measures, but to ensure that their implementation remains compatible with the protection of fundamental rights within the framework of a social and democratic State governed by the rule of law.

Keywords: Video surveillance; privacy; private life; data protection; security; fundamental rights; workplace.

1. Introducción

El aumento día a día de distintos sistemas de videovigilancia en el ámbito laboral y en los espacios de acceso público se ha convertido en uno de los fenómenos más significativos y controvertidos del derecho contemporáneo en materia de derechos fundamentales. El avance de la tecnología, la reducción de costes de los dispositivos de grabación y almacenamiento de imágenes y la creciente demanda de seguridad y control han impulsado el uso de estos sistemas, tanto por parte de las empresas como de quienes gestionan los espacios abiertos al público. Sin embargo, el uso de estas herramientas conlleva algunas implicaciones jurídicas, relacionadas principalmente con el derecho a la intimidad y con la protección de datos personales.

La seguridad es un valor esencial en las sociedades democráticas pues garantiza la convivencia, el orden público y la protección de personas y bienes. Por este motivo, la videovigilancia poco a poco se ha ido consolidando como un recurso eficaz para prevenir actos ilícitos, investigar conductas irregulares y proteger el patrimonio empresarial. No obstante, un uso indiscriminado o desproporcionado puede invadir la esfera privada de las personas, afectando no solo a los trabajadores sujetos al control empresarial, sino también a clientes, usuarios y terceros que acceden a espacios vigilados.

El conflicto entre seguridad y privacidad no ha surgido ahora, pero en la actualidad se ha intensificado mucho en los contextos laborales porque allí coincide la necesidad del empresario de organizar y supervisar la actividad productiva con los derechos fundamentales de los trabajadores, que no desaparecen por el hecho de estar en una relación laboral. Esta tensión exige una constante revisión, en la que el marco legal debe establecer límites claros y garantías efectivas que eviten sacrificar la intimidad en nombre de la eficiencia o la seguridad.

Desde una perspectiva constitucional, el artículo 18 de la Constitución española (CE) reconoce el derecho a la intimidad personal y familiar, así como el derecho fundamental a la protección de datos, constituyendo un núcleo de garantías frente a intromisiones ilegítimas en la vida privada. Este marco se ha reforzado y desarrollado tanto por la jurisprudencia del Tribunal Constitucional (TC) como por la normativa europea, especialmente desde que el derecho a la protección de datos se consagró como un derecho fundamental autónomo y de aplicación directa.

A nivel europeo, la evolución desde la Directiva 95/46/CE hasta el Reglamento general de protección de datos (RGPD) ha supuesto un cambio significativo en la concepción del tratamiento de datos personales. Se han introducido principios como la responsabilidad proactiva, la minimización de datos y la protección desde el diseño y por defecto, lo que ha tenido un impacto directo en los sistemas de videovigilancia, obligando a replantear su diseño, finalidad y uso, así como a reforzar los derechos de información y control de los sujetos afectados.

La jurisprudencia ha desempeñado un papel decisivo en la delimitación de los contornos de este equilibrio. En particular, los tribunales han ido perfilando los criterios que permiten determinar cuándo la videovigilancia constituye una medida legítima y proporcionada y cuándo, por el contrario, vulnera derechos fundamentales. Resulta especialmente relevante la doctrina del Tribunal Europeo de Derechos Humanos (TEDH), que ha abordado esta problemática desde la óptica del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo de derechos humanos. El conocido caso *López Ribalda y otros contra España* (2019)¹ ha marcado un punto de inflexión en la interpretación de la videovigilancia encubierta en el ámbito laboral, generando un intenso debate doctrinal y jurisprudencial sobre los límites del control empresarial.

En el ámbito interno, tanto el TC como el Tribunal Supremo (TS) han desarrollado una doctrina consolidada sobre la necesidad de respetar los principios de proporcionalidad, idoneidad y necesidad al adoptar medidas de control, así como la obligación de informar previamente a trabajadores y usuarios sobre la existencia de sistemas de videovigilancia. La Agencia española de protección de datos (AEPD) ha complementado este marco, concretando las obligaciones de los responsables del tratamiento y reforzando la tutela administrativa de los derechos fundamentales afectados.

En este contexto complejo y en constante cambio, resulta necesario un análisis crítico del marco jurídico de la videovigilancia en el ámbito laboral y comercial, identificando tanto avances como carencias en la protección de la intimidad frente a las crecientes

¹ Tribunal Europeo de Derechos Humanos, asunto *López Ribalda y otros c. España*, Gran Sala, de 17 de octubre de 2019. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-189675%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-189675%22]})

demandas de seguridad. No se busca cuestionar la legitimidad de las medidas de control, sino garantizar que su aplicación respete los principios constitucionales y la dignidad y autonomía personal de los individuos.

Este trabajo se sitúa precisamente en esa línea de reflexión, y trata de analizar el equilibrio entre seguridad y derecho a la intimidad desde la perspectiva constitucional, laboral y europea. Mediante el análisis normativo, jurisprudencial y doctrinal, se tratará de ofrecer una visión integral de los límites jurídicos de la videovigilancia y de las garantías necesarias para su uso legítimo. Además, también se tratará de proponer un modelo de videovigilancia que respete la privacidad y concilie de manera efectiva las exigencias de control y seguridad con la protección de los derechos fundamentales de trabajadores y usuarios en un entorno cada vez más digitalizado.

1.1 Justificación

La elección del tema de este trabajo tiene que ver con el aumento del uso de sistemas de videovigilancia en el ámbito laboral y en los establecimientos abiertos al público que hemos mencionado especialmente, por el impacto directo que estas prácticas tienen sobre derechos fundamentales tan importantes como el derecho a la intimidad y la protección de datos personales. La revolución tecnológica y el refuerzo de las exigencias de seguridad hacen urgente un análisis jurídico actualizado que permita delimitar los límites constitucionales y legales del control empresarial y de las medidas de seguridad privada, especialmente a la luz de la reciente jurisprudencia nacional y europea.

Además, la relevancia social y práctica de esta materia, unida a la dificultad de conciliar intereses enfrentados, pone de manifiesto la necesidad de un análisis sistemático que permita aclarar el marco jurídico aplicable y aportar criterios útiles para una aplicación respetuosa de los derechos fundamentales

1.2 Objetivos

El objetivo general del trabajo es analizar el equilibrio entre las exigencias de seguridad y el derecho a la intimidad en el uso de sistemas de videovigilancia en los ámbitos laboral y comercial.

Los objetivos específicos son:

- Examinar el marco constitucional, legal y europeo del derecho a la privacidad y la protección de datos.
- Analizar los límites jurídicos del control empresarial mediante videovigilancia.
- Estudiar la doctrina jurisprudencial más relevante en esta materia.
- Proponer un modelo de videovigilancia respetuoso con la privacidad y los derechos fundamentales.

1.3 Metodología

La metodología empleada se basa en una revisión bibliográfica de doctrina científica y normativa aplicable, así como en el análisis crítico de la jurisprudencia del TC, el TS, el TEDH y de las resoluciones de la AEPD, con el fin de extraer conclusiones sistemáticas y propuestas de mejora.



2. Marco teórico

2.1. El derecho fundamental a la privacidad

2.1.1. Concepto de privacidad y distinción frente a intimidad

El derecho a la privacidad constituye una de las manifestaciones más relevantes de la protección jurídica de la persona frente a las injerencias externas en su esfera personal. Aunque en el lenguaje jurídico español los términos “privacidad” e “intimidad” se han utilizado en ocasiones de forma indistinta, la doctrina ha subrayado la necesidad de diferenciarlos conceptualmente, especialmente a partir del desarrollo del derecho a la protección de datos personales.

Tradicionalmente, el derecho a la intimidad se ha entendido como el ámbito reservado de la vida personal y familiar que cada individuo decide sustraer al conocimiento ajeno, vinculado estrechamente a la dignidad de la persona (Martínez de Pisón, 2016).

La privacidad, por su parte, presenta un contenido más amplio y dinámico, que no se limita a los aspectos estrictamente íntimos, sino que abarca el control sobre la información personal y sobre las condiciones en que esta es recogida, tratada y difundida (Aragón Reyes, 2011).

El Tribunal Supremo, en la STS 398/2024², con el fin de diferenciar semánticamente los conceptos de “privacidad” e “intimidad”, acude al Diccionario de la Real Academia Española, donde la “privacidad” se define como el “ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión” y la “intimidad” como la “zona espiritual, íntima y reservada de una persona o de un grupo, especialmente de una familia” (Real Academia Española, s.f.).

Desde una perspectiva jurídica, el TC ha señalado que el derecho a la intimidad personal y familiar, reconocido en el artículo 18.1 de la CE, garantiza la existencia de un ámbito propio y reservado frente a la acción y conocimiento de terceros, imprescindible para el libre desarrollo de la personalidad (STC 231/1988³).

² Tribunal Supremo, Sala de lo Civil, STS 398/2024, de 19 de marzo. <https://vlex.es/vid/1028504074>

³ Tribunal Constitucional, STC 231/1988, de 2 de diciembre. <https://www.boe.es/buscar/doc.php?id=BOE-T-1988-29203>

En este contexto, la intimidad se configura como el núcleo más protegido de la vida personal, referido a aquellos aspectos especialmente sensibles que el individuo desea sustraer del conocimiento ajeno. Por su parte, la privacidad presenta un alcance más amplio, abarcando el conjunto de ámbitos de la vida personal que, sin pertenecer necesariamente a la esfera más íntima, deben quedar igualmente protegidos frente a injerencias externas. De este modo, puede afirmarse que la intimidad constituye una categoría cualificada dentro de la privacidad, caracterizada por un mayor nivel de protección jurídica.

Esta concepción encuentra también respaldo en el ámbito europeo, donde el artículo 8 del Convenio Europeo de Derechos Humanos reconoce el derecho al respeto de la vida privada y familiar. El Tribunal Europeo de Derechos Humanos ha interpretado este concepto de forma amplia, incluyendo no sólo los aspectos más íntimos de la persona, sino también otros elementos de su vida privada, como su identidad personal, sus relaciones sociales o su desarrollo en el ámbito profesional.

En consecuencia, la doctrina europea refuerza la idea de que la privacidad constituye un concepto más extenso, dentro del cual la intimidad representa su dimensión más restringida y especialmente protegida, lo que justifica un mayor grado de exigencia en la legitimación de cualquier injerencia en este ámbito.

Finalmente, resulta necesario situar los conceptos de privacidad e intimidad en relación con otros derechos de la personalidad reconocidos en el artículo 18 de la CE, como el derecho al honor y a la propia imagen. Si bien estos derechos comparten una misma finalidad de protección de la esfera personal del individuo, presentan un contenido diferenciado. Así, el derecho a la intimidad protege el ámbito reservado de la vida personal y familiar, mientras que el derecho al honor se vincula con la reputación y la consideración social de la persona, y el derecho a la propia imagen garantiza el control sobre la captación, reproducción y difusión no solo de los rasgos físicos identificativos, sino también de aquellos elementos de carácter personal o identitario, como la voz, la gestualidad, la apariencia externa, los signos distintivos o cualquier otro rasgo singular, que, permitan la identificación directa o indirecta de la persona..

De este modo, aunque todos ellos integran el núcleo de derechos de la personalidad, la intimidad se distingue por referirse al ámbito más interno y reservado del individuo, lo que justifica un nivel de protección particularmente intenso frente a injerencias externas.

Esta concepción amplia resulta especialmente relevante en contextos como el laboral o establecimientos abiertos al público, donde las personas desarrollan actividades que, sin pertenecer al núcleo más íntimo de su vida personal, forman parte de su esfera privada y, por tanto, merecen protección frente a injerencias externas, especialmente cuando se materializan a través de mecanismos intensivos de vigilancias o control tecnológico.

2.1.2. Evolución histórica del derecho a la privacidad

El reconocimiento jurídico del derecho a la privacidad es relativamente reciente y se encuentra estrechamente ligado a los cambios sociales y tecnológicos de las sociedades contemporáneas. Uno de los hitos fundamentales en su formulación moderna es el célebre artículo de Warren y Brandeis, *The Right to Privacy* (1890), en el que se reivindica el “*right to be let alone*”⁴ como respuesta a las intromisiones derivadas del desarrollo de los medios de comunicación de la época.

En el ámbito europeo, la protección de la vida privada se consolida tras la Segunda Guerra Mundial, especialmente a través del artículo 8 del CEDH que reconoce el derecho al respeto de la vida privada y familiar. A partir de este reconocimiento, la privacidad deja de concebirse como un derecho meramente negativo y pasa a configurarse como un derecho que exige garantías positivas por parte de los poderes públicos (Pérez de los Cobos Orihuel, 2018).

La progresiva informatización de la sociedad y el tratamiento masivo de datos personales han impulsado una evolución adicional del concepto, dando lugar al reconocimiento del derecho a la protección de datos como una dimensión específica y autónoma de la privacidad.

2.1.3. Tratamiento constitucional en el artículo 18 de la CE

En el ordenamiento jurídico español, el derecho a la intimidad encuentra su principal anclaje constitucional en el artículo 18.1 de la CE, que garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este precepto configura un ámbito de protección frente a intromisiones ilegítimas tanto de los poderes públicos como de los particulares.

⁴ Derecho a ser dejado solo.

La jurisprudencia del TC ha destacado reiteradamente que el derecho a la intimidad protege un espacio de vida personal inmune a la curiosidad ajena, incluso en contextos en los que el individuo se relaciona con terceros, como ocurre en el ámbito laboral (STC 98/2000⁵; STC 186/2000⁶). En este sentido, el alto Tribunal ha afirmado que la celebración de un contrato de trabajo no implica una renuncia a los derechos fundamentales del trabajador, sino únicamente una modulación de su ejercicio en atención a las exigencias de la relación laboral.

Asimismo, el artículo 18.4 CE introduce una garantía específica frente al uso de la informática, anticipando la necesidad de limitar el tratamiento automatizado de datos personales para preservar la intimidad y los derechos fundamentales. Este precepto ha sido clave en la posterior construcción del derecho fundamental a la protección de datos.

2.1.4. La protección de datos como derecho fundamental autónomo

El TC ha reconocido de forma expresa la autonomía del derecho fundamental a la protección de datos personales, diferenciándolo del derecho a la intimidad. En su conocida STC 292/2000⁷, el Tribunal afirma que este derecho otorga a su titular un poder de disposición y control sobre sus datos personales, permitiéndole conocer quién los posee, con qué finalidad y exigir, en su caso, su rectificación o cancelación.

Esta configuración resulta especialmente relevante en el ámbito de la videovigilancia, donde el tratamiento de imágenes implica la captación y conservación de datos personales, incluso cuando no se refieran a aspectos íntimos de la vida del individuo. La protección ya no se limita al contenido de la información, sino que se extiende a las condiciones mismas del tratamiento (Gil Membrado, 2019).

⁵ Tribunal Constitucional, STC 98/2000, de 10 de abril. https://www.boe.es/diario_boe/txt.php?id=BOE-T-2000-9223

⁶ Tribunal Constitucional, STC 186/2000, de 10 de julio. https://www.boe.es/diario_boe/txt.php?id=BOE-T-2000-15253

⁷ Tribunal Constitucional, STC 292/2000, de 30 de noviembre. <https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276>

De este modo, prácticas que tradicionalmente se consideraban neutras desde la perspectiva de la intimidad adquieren relevancia constitucional cuando implican un tratamiento sistemático y tecnológico de datos personales.

2.1.5. La perspectiva europea: de la Directiva 95/46/CE al RGPD

La consolidación del derecho a la protección de datos ha venido acompañada de un papel decisivo del derecho de la Unión Europea (UE). La Directiva 95/46/CE fue el primer intento de establecer un marco normativo común en esta materia, fijando principios esenciales como la calidad de los datos, la limitación de la finalidad del tratamiento y el reconocimiento de los derechos de los interesados.

Sin embargo, con la entrada en vigor del Reglamento (UE) 2016/679, general de protección de datos, es cuando se produce un avance importante en el nivel de protección. El RGPD reconoce de forma expresa la protección de datos como un derecho fundamental, de conformidad con el artículo 8 de la Carta de derechos fundamentales de la UE, y refuerza de manera significativa las obligaciones de los responsables del tratamiento a través de principios como la responsabilidad proactiva y la protección de datos desde el diseño y por defecto.

En el ámbito específico de la videovigilancia, estas exigencias implican la necesidad de justificar con mayor rigor la legitimidad, proporcionalidad y necesidad de los sistemas de control visual, así como de garantizar de forma efectiva los derechos de información y transparencia tanto de los trabajadores como de los usuarios.

2.1.6. Privacidad, dignidad y autonomía personal

Finalmente, el derecho a la privacidad no puede entenderse de forma aislada, sino en estrecha conexión con la dignidad de la persona y su autonomía personal. La vigilancia constante o intensiva puede generar efectos disuasorios sobre la libertad de comportamiento y la autodeterminación individual, incluso cuando no se produzcan intromisiones directas en la intimidad más estricta (Velásquez Espinoza, G. E., y Román Armijos, R.A., 2024).

2.2. La seguridad y el control en las relaciones laborales y en los establecimientos abiertos al público

2.2.1. La seguridad como bien jurídico y función del Estado

La seguridad constituye uno de los bienes jurídicos de mayor densidad estructural dentro del Estado constitucional, aunque su ubicación sistemática no sea la de un derecho fundamental subjetivo. En el texto constitucional español, la seguridad aparece formulada de manera fragmentaria, asociada tanto a la garantía del orden público como a la protección de personas y bienes, y confiada de forma primordial a la actuación de los poderes públicos (art. 104 CE).

El Tribunal Constitucional ha subrayado que la seguridad no puede concebirse como un fin autónomo desligado del sistema de derechos, sino como una condición instrumental para su ejercicio efectivo. En este sentido, ha advertido que la invocación genérica de la seguridad no legitima por sí misma restricciones intensas de derechos fundamentales, siendo necesaria una justificación específica y ponderada en cada caso concreto (STC 341/1993⁸). La seguridad, por tanto, opera como un bien constitucionalmente relevante, pero estructuralmente subordinado al principio de proporcionalidad.

Desde una perspectiva doctrinal, se ha puesto de relieve el carácter ambivalente de la seguridad en las democracias contemporáneas: al tiempo que resulta imprescindible para garantizar la convivencia social, su expansión ilimitada puede erosionar las bases mismas del Estado de derecho (Ferrajoli, 2011). Esta tensión se intensifica cuando la seguridad deja de ser una función ejercida exclusivamente por el Estado y comienza a desplegarse mediante mecanismos privados de control.

2.2.2. Seguridad privada, control empresarial y prevención de ilícitos

La progresiva externalización y privatización de funciones vinculadas a la seguridad constituye uno de los rasgos más característicos de las sociedades contemporáneas. Empresas de seguridad privada, sistemas tecnológicos de control y mecanismos

⁸ Tribunal Constitucional, STC 341/1993, de 18 de noviembre.

<https://www.boe.es/buscar/doc.php?id=BOE-T-1993-29248>

automatizados de vigilancia operan hoy de forma cotidiana en espacios tradicionalmente ajenos al control permanente, configurando un entramado de supervisión difusa difícilmente perceptible para los sujetos afectados.

Este fenómeno encuentra su encaje jurídico en el marco de la Ley 5/2014, de 4 de abril, de Seguridad Privada, que regula la prestación por entidades privadas de servicios de vigilancia y protección de bienes, establecimientos y eventos, así como el control de accesos y otras actuaciones orientadas a la prevención de riesgos. La norma delimita tanto las funciones atribuidas al sector como los límites de su actuación.

Dicha ley reconoce la legitimidad de estas actividades en cuanto contribuyen a la seguridad pública. No obstante, tales funciones no pueden confundirse con el ejercicio de potestades públicas propias de las Fuerzas y Cuerpos de Seguridad, quedando sometidas a límites estrictos de actuación, habilitación profesional y control administrativo. En este sentido, la propia norma subraya el carácter complementario y subordinado de la seguridad privada respecto de la seguridad pública.

Especial relevancia adquiere el uso de medios tecnológicos de seguridad, entre ellos los sistemas de videovigilancia, cuya utilización debe responder a finalidades legítimas y respetar no solo la normativa sectorial de seguridad privada, sino también el régimen general de protección de datos personales y la doctrina constitucional relativa a la proporcionalidad de las injerencias en derechos fundamentales.

En el ámbito empresarial, la seguridad se articula frecuentemente en términos de prevención de ilícitos, protección del patrimonio y reducción de riesgos económicos. Estas finalidades, legítimas en sí mismas, han servido de fundamento para la implantación de medidas de control cada vez más sofisticadas, entre las que destaca el recurso a tecnologías de captación y tratamiento de imágenes. No obstante, la propia normativa de seguridad privada exige que estas medidas se desarrollen con pleno respeto al ordenamiento jurídico y a los derechos fundamentales. En este sentido, la Ley 5/2014 de Seguridad Privada establece que los servicios de seguridad privada tienen carácter complementario y subordinado respecto de la seguridad pública, debiendo ejercerse con sujeción a la legalidad vigente y con respeto a los derechos fundamentales. Por ello, el uso de sistemas de vigilancia, especialmente aquellos basados en la captación y tratamiento de imágenes, debe ajustarse a los principios de legalidad y proporcionalidad, conforme a la normativa de protección de datos personales RGPD, Ley Orgánica 3/2018 y a la doctrina constitucional.

La normalización del control tecnológico plantea, además, un desplazamiento significativo del eje de la vigilancia: ya no se trata únicamente de reaccionar frente a conductas ilícitas, sino de anticiparlas, detectarlas o incluso disuadirlas mediante la mera presencia de sistemas de control. Esta lógica preventiva, característica de lo que parte de la doctrina ha denominado “sociedad de la vigilancia”, introduce riesgos estructurales para la libertad individual y la autonomía personal (Zuboff, 2019). En este contexto, diversos autores advierten que la generalización de estos mecanismos puede derivar en un escenario de vigilancia permanente, en el que la conducta de los individuos se ve condicionada por la posibilidad constante de ser observados, lo que altera sustancialmente la esencia misma de la libertad humana. Todo ello exige reforzar los mecanismos de control jurídico sobre el uso de estas tecnologías.

2.2.3. El poder de dirección y control del empresario (art. 20.3 ET)

En el marco de las relaciones laborales, el poder de control del empresario encuentra su principal fundamento normativo en el artículo 38 CE relativo a la libertad de empresa, otorgando al empresario la capacidad de organizar, dirigir y supervisar la actividad productiva para garantizar la eficiencia y la seguridad de su organización; y el artículo 20.3 del Estatuto de los Trabajadores, que le habilita para adoptar las medidas de vigilancia y control necesarias para verificar el cumplimiento de las obligaciones laborales. Se trata de una habilitación amplia, formulada en términos deliberadamente abiertos, pero condicionada expresamente al respeto de la dignidad del trabajador.

La jurisprudencia constitucional ha insistido en que el contrato de trabajo no puede operar como un mecanismo de desconstitucionalización de la relación laboral. La celebración de un contrato de trabajo no implica la renuncia de la persona empleada a sus derechos fundamentales, como la intimidad -artículo 18.1 CE- o la protección de datos -artículo 18.4 CE-. Los derechos fundamentales acompañan al trabajador dentro de la empresa, aunque su ejercicio pueda verse modulable en atención a las exigencias organizativas y productivas (STC 98/2000). Esta modulación, sin embargo, no equivale a una disponibilidad plena por parte del empleador.

En este escenario, el TC (STC 119/2022⁹) ha dictaminado que no puede reprocharse a una empresa el uso de grabaciones audiovisuales cuando existan sospechas fundadas de un comportamiento infractor por parte de la persona empleada. Sin embargo, para que el ejercicio de este poder derivado de la libertad de empresa no degenera en un control arbitrario, la doctrina y la jurisprudencia exigen que cualquier medida de videovigilancia supere el triple juicio de proporcionalidad:

Idoneidad: que la medida sea capaz de lograr el objetivo de supervisión o seguridad.

Necesidad: que no existan otros medios menos intrusivos e igualmente eficaces.

Proporcionalidad en sentido estricto: que el beneficio obtenido para la empresa sea superior al sacrificio que se impone a la privacidad del trabajador.

Por tanto, el marco constitucional actual sitúa la videovigilancia no solo como un medio técnico, sino como una herramienta de poder inserta en una relación de asimetría estructural.

Desde la doctrina laboralista se ha destacado que el verdadero problema del control empresarial no radica en su existencia, sino en su intensidad y en su carácter potencialmente invasivo cuando se apoya en tecnologías que permiten una supervisión constante y sistemática (Álvarez de la Rosa y Palomeque López, 2022). La introducción de sistemas de videovigilancia altera cualitativamente las condiciones de prestación del trabajo, generando un entorno de observación permanente que puede incidir en la libertad de comportamiento del trabajador.

2.2.4. La prevención de pérdidas y riesgos en comercios y espacios de acceso público

En los establecimientos abiertos al público, la seguridad se vincula de forma directa a la prevención de pérdidas, la protección de bienes y la garantía de la integridad de clientes y empleados. El recurso a sistemas de videovigilancia se presenta habitualmente como una respuesta eficaz frente a fenómenos como el hurto, el vandalismo o las agresiones, especialmente en sectores comerciales con alta afluencia de público.

⁹ Tribunal Constitucional, STC 119/2022, de 29 de septiembre.

<https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/29082>

Ahora bien, la apertura del espacio al público no implica la desaparición de toda expectativa razonable de privacidad. El Tribunal Constitucional ha señalado que la protección del derecho a la intimidad no se agota en el ámbito estrictamente doméstico, pudiendo proyectarse sobre espacios de interacción social cuando la intensidad del control así lo exige (STC 186/2000). La condición de cliente o usuario no convierte al individuo en un sujeto desprovisto de garantías frente a la vigilancia.

Desde la perspectiva de la protección de datos, la captación sistemática de imágenes en estos espacios constituye un tratamiento de datos personales que debe someterse a los principios de finalidad, minimización y proporcionalidad. La Agencia Española de Protección de Datos ha insistido reiteradamente en que la finalidad preventiva no justifica por sí sola una vigilancia indiscriminada o permanente de zonas no estrictamente necesarias para la seguridad (AEPD, 2025).

2.2.5. Límites constitucionales y legales al control mediante videovigilancia

El denominador común de las distintas manifestaciones del control mediante videovigilancia es la necesidad de someter su utilización a límites constitucionales y legales estrictos. La jurisprudencia ha construido un canon consolidado de enjuiciamiento basado en el principio de proporcionalidad, que exige verificar la idoneidad, necesidad y proporcionalidad en sentido estricto de la medida adoptada (STC 29/2013¹⁰).

A ello se suma la exigencia de transparencia e información previa, especialmente relevante en el ámbito laboral, donde la posición de subordinación del trabajador intensifica el deber de garantía por parte del empleador. La ausencia de información adecuada ha sido considerada por el TC y por el TEDH como un elemento determinante en la apreciación de vulneraciones del derecho a la vida privada (*asunto López Ribalda y otros contra España*, 17 de octubre de 2019).

En definitiva, el control mediante videovigilancia sólo resulta constitucionalmente legítimo cuando se inserta en un marco normativo claro, responde a finalidades concretas y legítimas, y se aplica de forma proporcionada y respetuosa con la dignidad y los

¹⁰ Tribunal Constitucional, STC 29/2013, de 11 de febrero.
<https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/23284>

derechos fundamentales de las personas afectadas. Cualquier desviación de estos parámetros convierte la seguridad en un pretexto incompatible con los valores del Estado constitucional de derecho.

2.3. La videovigilancia laboral y en establecimientos abiertos al público

2.3.1. Concepto y tipologías: videovigilancia laboral, comercial y en comunidades de propietarios

Desde una perspectiva jurídica, la videovigilancia puede definirse como el conjunto de técnicas y sistemas destinados a la captación, grabación, transmisión o almacenamiento de imágenes de personas identificadas o identificables con fines de seguridad, control o supervisión. Esta definición, aparentemente neutra, adquiere una relevancia constitucional inmediata cuando la captación de imágenes se integra en un tratamiento sistemático de datos personales.

El TC ha señalado que la grabación de imágenes constituye una forma de tratamiento de datos personales cuando permite identificar directa o indirectamente a las personas afectadas, con independencia de que se refiera o no a aspectos íntimos de su vida (STC 292/2000). La relevancia jurídica de la videovigilancia no deriva, por tanto, del contenido de la imagen en sí, sino del contexto tecnológico y funcional en el que se inserta.

La doctrina (Ferrajoli, 2011) (Baylos Grau, 2019) (Álvarez de la Rosa y Palomeque López, 2022) ha subrayado que la videovigilancia no puede analizarse como un mero medio técnico de observación, sino como una herramienta de poder capaz de alterar las condiciones de libertad y autonomía de los individuos sometidos a ella. En el ámbito laboral y en los espacios abiertos al público, esta capacidad se ve reforzada por la asimetría estructural existente entre quien controla el sistema y quien es objeto de la vigilancia.

Desde esta óptica, la videovigilancia se sitúa en una zona de fricción permanente entre la eficacia preventiva y la protección de los derechos fundamentales, exigiendo un análisis jurídico particularmente cuidadoso.

Desde el punto de vista jurídico, resulta necesario distinguir entre distintas tipologías de videovigilancia en función de su finalidad, del espacio en el que se desarrolla y de los

sujetos afectados. Esta diferenciación no es meramente descriptiva, sino que condiciona el juicio de legitimidad constitucional de la medida.

Una primera distinción clásica separa la videovigilancia con fines de seguridad general (orientada a la protección de personas y bienes) de aquella destinada específicamente al control del cumplimiento de obligaciones laborales o contractuales. Mientras que en el primer caso la finalidad preventiva suele gozar de un mayor reconocimiento, en el segundo se intensifican las exigencias de justificación y proporcionalidad (Álvarez de la Rosa y Palomeque López, 2022).

Asimismo, cabe diferenciar entre videovigilancia en espacios cerrados de acceso restringido y aquella desplegada en establecimientos abiertos al público. En estos últimos, aunque la expectativa de privacidad pueda considerarse menor, no desaparece por completo, especialmente cuando la vigilancia es permanente o afecta a zonas no directamente vinculadas a la finalidad de seguridad (STC 186/2000).

Finalmente, la doctrina distingue entre sistemas de grabación continua y sistemas activados por eventos concretos, siendo estos últimos generalmente considerados menos intrusivos desde la perspectiva del principio de minimización de datos.

2.3.2. Finalidades legítimas: control laboral, seguridad, prevención de delitos y protección del patrimonio

La consideración de la videovigilancia como tratamiento de datos personales se encuentra plenamente consolidada tanto en el derecho europeo como en el ordenamiento interno. El Reglamento General de Protección de Datos (RGPD) incluye expresamente las imágenes de personas físicas entre los datos personales cuando permitan su identificación, directa o indirecta (art. 4.1 RGPD).

Esta calificación comporta consecuencias jurídicas relevantes. En primer lugar, somete los sistemas de videovigilancia a los principios generales del tratamiento de datos, entre los que destacan la licitud, la limitación de la finalidad, la minimización de datos y la limitación del plazo de conservación. En segundo lugar, impone obligaciones específicas al responsable del tratamiento, especialmente en materia de información, seguridad y responsabilidad proactiva (art. 5 y 24 RGPD).

La Agencia Española de Protección de Datos ha insistido en que la captación continua de imágenes constituye una forma particularmente intensa de tratamiento, precisamente

por su carácter potencialmente indiscriminado y por la dificultad de control efectivo por parte de los interesados (AEPD, 2025). Esta intensidad explica que la videovigilancia se encuentre sometida a un estándar reforzado de proporcionalidad.

No resulta irrelevante, además, que el tratamiento de imágenes permita usos secundarios o desviados, como el análisis de comportamientos o la elaboración de perfiles, lo que incrementa los riesgos para los derechos fundamentales cuando no existen garantías suficientes (Bygrave, 2014).

Ahora bien, la legitimidad del uso de sistemas de videovigilancia depende en gran medida de la finalidad perseguida, siendo generalmente admitidas aquellas vinculadas al control laboral, la seguridad, la prevención de delitos y la protección del patrimonio.

En el ámbito laboral, la videovigilancia encuentra su fundamento en el poder de dirección y control del empresario reconocido en el artículo 20.3 del Estatuto de los Trabajadores. No obstante, este poder no es ilimitado, sino que debe ejercerse respetando los derechos fundamentales de los trabajadores, en particular el derecho a la intimidad y a la protección de datos personales. La jurisprudencia constitucional ha reconocido que el tratamiento de datos personales exige garantizar el control por parte del individuo sobre su información personal, configurando un derecho autónomo diferenciado del derecho a la intimidad, tal como establece la STC 292/2000. En la misma línea, la jurisprudencia del TEDH ha señalado que la videovigilancia encubierta sólo puede considerarse legítima en supuestos excepcionales, cuando concurren sospechas razonables y la medida supere un estricto juicio de proporcionalidad, como se recoge en el asunto López Ribalda y otros contra España (7 de octubre de 2019).

Por otro lado, la videovigilancia con fines de seguridad y prevención de delitos constituye una de las finalidades más habituales, especialmente en establecimientos abiertos al público, infraestructuras y espacios de acceso público. En estos supuestos, el tratamiento puede ampararse en el interés legítimo del responsable o en el cumplimiento de una misión realizada en interés público. No obstante, la mera invocación de la seguridad no legitima cualquier forma de vigilancia, siendo necesario acreditar que la medida resulta idónea para el fin perseguido, necesaria en ausencia de alternativas menos intrusivas y proporcionada en sentido estricto.

En relación con la protección del patrimonio, la videovigilancia se configura como un instrumento preventivo frente a conductas como robos, hurtos o actos vandálicos. Sin

embargo, esta finalidad tampoco justifica una captación indiscriminada o excesiva de imágenes, debiendo limitarse a los espacios estrictamente necesarios y evitando la grabación de zonas especialmente protegidas, como vestuarios, aseos o espacios destinados al descanso de los trabajadores.

En este sentido, la legitimidad de cualquiera de estas finalidades se encuentra condicionada al cumplimiento del denominado juicio de proporcionalidad, que exige verificar que la medida adoptada sea adecuada para alcanzar el objetivo perseguido, necesaria en ausencia de medidas menos invasivas y equilibrada en relación con los derechos afectados.

Finalmente, la creciente incorporación de tecnologías avanzadas, como los sistemas de análisis automatizado de imágenes o el reconocimiento facial, intensifica los riesgos asociados a la videovigilancia, al permitir la elaboración de perfiles o la inferencia de comportamientos. Esta circunstancia exige un escrutinio aún más riguroso de la finalidad del tratamiento y refuerza la necesidad de establecer garantías adicionales que aseguren el respeto a los derechos fundamentales.

2.3.3. Videovigilancia manifiesta y encubierta

Una de las distinciones más relevantes, tanto doctrinal como jurisprudencialmente, es la que separa la videovigilancia visible de la videovigilancia encubierta. La primera se caracteriza por la existencia de información previa clara y accesible sobre la instalación de cámaras, mientras que la segunda implica la ocultación deliberada del sistema de grabación respecto de las personas afectadas.

La videovigilancia visible se ha considerado, con carácter general, compatible con el ordenamiento jurídico siempre que respete los principios de proporcionalidad y transparencia. La obligación de información previa constituye aquí una garantía esencial, no solo desde la perspectiva de la protección de datos, sino también como límite al efecto disuasorio excesivo de la vigilancia (STC 29/2013).

Por el contrario, la videovigilancia encubierta ha sido objeto de un escrutinio mucho más estricto. El Tribunal Europeo de Derechos Humanos ha señalado que la ausencia de información previa supone una injerencia especialmente intensa en el derecho al respeto

de la vida privada, que sólo puede justificarse en circunstancias excepcionales y bajo criterios muy rigurosos (*Köpke c. Alemania*, 5 de octubre de 2010¹¹).

El caso *López Ribalda y otros c. España* (17 de octubre de 2019) ha reabierto este debate, al admitir la legitimidad de cámaras ocultas en un contexto de sospechas graves y fundadas de conductas ilícitas, pero subrayando al mismo tiempo el carácter excepcional de esta medida. No obstante, la sentencia ha sido objeto de intensas críticas doctrinales, en la medida en que parte de la doctrina considera que el Tribunal flexibiliza en exceso las exigencias de información previa al trabajador y de transparencia en el tratamiento de datos personales. En particular, se ha señalado que la admisión de medidas de videovigilancia encubierta, aun en supuestos excepcionales, puede abrir la puerta a una utilización más amplia de este tipo de controles en el ámbito laboral, debilitando las garantías del derecho a la intimidad y a la protección de datos. Asimismo, se advierte del riesgo de que esta interpretación contribuya a normalizar prácticas de vigilancia oculta, desplazando el estándar hacia modelos más permisivos y generando un efecto disuasorio en el comportamiento de los trabajadores, al actuar bajo la permanente posibilidad de ser observados sin su conocimiento (Baylos Grau, 2019).

2.3.4. Impacto social y riesgos específicos para la privacidad de trabajadores y clientes

La implantación de sistemas de videovigilancia no produce únicamente efectos jurídicos directos sobre los derechos individuales, sino que genera también consecuencias sociales más amplias que deben ser tenidas en cuenta en el análisis de su legitimidad. La vigilancia visual permanente, especialmente cuando se normaliza en contextos cotidianos como el trabajo o el consumo, altera de manera significativa las condiciones en las que las personas desarrollan su conducta y ejercen su autonomía.

En el ámbito laboral, diversos estudios han puesto de relieve que la percepción de estar siendo observado de forma constante puede generar efectos de autocensura, incremento del estrés y modificación del comportamiento frente a expectativas externas, incluso

¹¹ Tribunal Europeo de Derechos Humanos, asunto *Köpke c. Alemania*, decisión de 5 de octubre de 2010. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-101536%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-101536%22]})

cuando no existe un uso efectivo de las grabaciones con fines disciplinarios. La videovigilancia continuada no solo registra conductas, sino que puede condicionarlas, favoreciendo dinámicas de sobreadaptación a expectativas externas y reduciendo la autonomía percibida del trabajador.¹²

La videovigilancia actúa así como un mecanismo de control indirecto, capaz de intensificar la subordinación propia de la relación laboral más allá de los límites estrictamente necesarios para la organización productiva. Esta dimensión social del control ha sido destacada por la doctrina crítica, que advierte del riesgo de convertir el espacio de trabajo en un entorno de supervisión continua, incompatible con una concepción sustantiva de la dignidad del trabajador (Baylos Grau, 2019). En la misma línea, el Tribunal Constitucional, aunque no ha empleado expresamente esta terminología, ha reconocido que las medidas de vigilancia pueden afectar no solo al derecho a la intimidad, sino también al libre desarrollo de la personalidad cuando resultan innecesarias o desproporcionadas (STC 29/2013). La expectativa permanente de observación puede condicionar intensamente la conducta del empleado, limitar su espontaneidad relacional y reducir su autonomía personal. De este modo, la videovigilancia excesiva no solo supervisa comportamientos, sino que puede llegar a configurarlos, proyectando sus efectos sobre la libertad individual dentro de la relación de trabajo.

En el caso de los clientes y usuarios de establecimientos abiertos al público, los riesgos presentan características específicas. Aunque se trate de espacios en los que la expectativa de privacidad es menor, ello no implica la desaparición de toda protección. La captación sistemática de imágenes de clientes, asociada en ocasiones a finalidades de prevención de pérdidas o análisis de comportamientos, puede dar lugar a tratamientos masivos y difícilmente controlables por los afectados, especialmente cuando se emplean tecnologías avanzadas o sistemas de análisis de datos, lo que exige un estricto cumplimiento de los principios de proporcionalidad, minimización y limitación de la finalidad, pudiendo incluso generar riesgos significativos para los derechos y libertades de las personas cuando estos sistemas implican un tratamiento intensivo o sistemático de datos personales. (AEPD, *Guía sobre el uso de videocámaras para seguridad y otras finalidades*, 2025).

¹² Véase Ball, K. (2021). *Electronic Monitoring and Surveillance in the Workplace*. Joint Research Centre, Comisión Europea; Glavin, P. et al. (2024). *Workplace Surveillance and Worker Well-Being*.

Desde una perspectiva social, la generalización de la videovigilancia en comercios contribuye a la normalización de prácticas de control que afectan de forma indistinta a todos los usuarios, con independencia de la existencia de riesgos concretos. Esta lógica preventiva expansiva ha sido criticada por su potencial efecto estigmatizador y por el desplazamiento del principio de presunción de inocencia hacia un modelo de sospecha difusa.

A ello se añade el riesgo de usos secundarios de las imágenes, como su reutilización con fines distintos a los inicialmente declarados o su cesión indebida a terceros. La experiencia práctica demuestra que estos riesgos aumentan en contextos en los que la videovigilancia se integra en estrategias comerciales más amplias, como el análisis de flujos de clientes o la detección automatizada de comportamientos considerados anómalos (Bygrave, 2014).

La reacción de los usuarios depende en gran medida de la finalidad percibida, del nivel de información facilitado y de la intensidad tecnológica del sistema empleado. Cuando la videovigilancia se combina con mecanismos de reconocimiento facial, análisis biométrico o elaboración automatizada de perfiles, el grado de aceptación social disminuye de forma apreciable, al incrementarse la percepción de riesgo para la privacidad y para la libertad de circulación en espacios cotidianos.¹³

El impacto social de la videovigilancia se ve además intensificado por la asimetría informativa que caracteriza a estos sistemas. Tanto trabajadores como clientes suelen desconocer el alcance real del tratamiento de sus imágenes, los plazos de conservación o las posibles interconexiones con otros sistemas de control, lo que debilita su capacidad de ejercer de manera efectiva los derechos reconocidos por la normativa de protección de datos.

Por todo lo que se acaba de señalar, el análisis jurídico de la videovigilancia no puede limitarse a una verificación formal de requisitos legales, sino que debe incorporar una evaluación minuciosa de todos sus efectos sociales que, además, se van acumulando.

Existen estudios que han concluido que la implantación masiva de sistemas de videovigilancia, tanto en el entorno laboral como en espacios de acceso público, genera transformaciones profundas en la convivencia y en la psicología individual.

¹³ Véase European Data Protection Board (2020). *Guidelines 3/2019 on processing of personal data through video devices*.

La implantación de sistemas de videovigilancia en el ámbito laboral no responde únicamente a objetivos de seguridad o control de la productividad, sino que también puede tener efectos relevantes en la salud mental de los trabajadores y en la dinámica organizativa de las empresas. La monitorización constante puede incrementar los niveles de estrés y ansiedad al generar la sensación de estar permanentemente observado, fenómeno que algunos autores relacionan con el denominado *tecno-estrés*. Esta situación puede derivar en fatiga emocional, pérdida de motivación e incluso sentimientos de alienación cuando la vigilancia se percibe como excesiva o injustificada.

En esta línea, la *Carta de Derechos Digitales (2021)*, insiste en que la transformación digital del trabajo debe respetar la dignidad, la intimidad y el bienestar de las personas trabajadoras.¹⁴ Como ha señalado Baylos Grau, A. (2019) las facultades empresariales de control no pueden ejercerse al margen de la dignidad de la persona trabajadora, pues la empresa no constituye un espacio inmune a los derechos fundamentales. Asimismo, Molina Navarrete, C. (2019) advierte que la gran transformación digital del trabajo exige reforzar la prevención frente a nuevos riesgos psicosociales derivados de formas intensivas de control tecnológico y pérdida de bienestar. Desde esta perspectiva, la digitalización del poder empresarial no puede desvincularse de límites orientados a proteger la salud mental, la autonomía personal y el libre desarrollo de la personalidad

Asimismo, el autor especializado en psicología laboral y control empresarial, como Ball (2010), sostiene que la percepción de vigilancia continua puede asociarse con una menor satisfacción laboral y un incremento del estrés ocupacional. La reducción de la autonomía en el desempeño del trabajo y el aumento de las presiones derivadas del control constante pueden llevar al trabajador a sentir que pierde el control sobre su propio ritmo de trabajo y su capacidad de decisión.

Desde una perspectiva organizativa, la utilización intensiva de estos sistemas puede favorecer un clima de sospecha en lugar de uno basado en la confianza regulada. Cuando la supervisión tecnológica se aproxima al micromanagement, puede afectar negativamente a la moral de los empleados y limitar su creatividad o iniciativa.

En un plano más amplio, la percepción de vigilancia permanente también puede provocar cambios en el comportamiento de las personas. Saber que se está siendo

¹⁴ *Carta de Derechos Digitales (2021)*, apartados relativos a los derechos digitales en el entorno laboral y a la protección de la persona en contextos digitalizados.

observado puede generar un efecto disuasorio que conduce a la autocensura y a la adaptación del comportamiento a lo que se considera socialmente esperado por el observador.

Paradójicamente, David Lyon (2001) sostiene que los sistemas de vigilancia intensiva pueden generar efectos contraproducentes en los individuos sometidos a supervisión constante, especialmente cuando dicha vigilancia es percibida como excesiva o invasiva, pudiendo favorecer dinámicas de desconfianza y resistencia frente al sistema de control.

En los espacios abiertos al público, la expansión de la videovigilancia ha ido acompañada de una creciente aceptación social de estos sistemas. Sin embargo, esta normalización puede reducir la percepción de intromisión en la vida privada y favorecer una aceptación poco crítica de tecnologías cada vez más sofisticadas de control y análisis del comportamiento.

Además, la evolución tecnológica está impulsando un desplazamiento desde modelos de vigilancia reactiva hacia sistemas de carácter preventivo o predictivo. Este cambio puede generar preocupaciones relacionadas con la posible instauración de una lógica de sospecha generalizada sobre ciudadanos y clientes.

Debe tenerse en cuenta la existencia de una asimetría significativa entre quienes gestionan estos sistemas y las personas sometidas a vigilancia. En muchos casos, los individuos desconocen el alcance real del tratamiento de sus imágenes o el uso de herramientas de análisis automatizado, lo que puede generar una situación de vulnerabilidad estructural en relación con el control de su propia información personal. Esta circunstancia pone de manifiesto la necesidad de reforzar no solo las garantías jurídicas existentes, sino también la formación y capacitación digital de los ciudadanos, permitiéndoles comprender de manera más clara cómo funcionan estos sistemas, qué derechos les asisten y cuáles son los límites legales aplicables al tratamiento de sus datos personales.

En conclusión, la videovigilancia no es una herramienta neutra; su presencia constante puede transformar entornos de confianza en espacios de vigilancia algorítmica donde la libertad individual se ve condicionada por el diseño digital del control. La protección de la privacidad frente a estos sistemas exige atender no solo a la existencia de una base jurídica, sino también al impacto real que la vigilancia continuada produce sobre las condiciones de libertad y confianza que caracterizan a una sociedad democrática.

2.4. Límites jurídicos de la videovigilancia en el ámbito laboral y comercial

La delimitación jurídica de la videovigilancia en el ámbito laboral y en los establecimientos abiertos al público se desarrolla a partir de un entramado normativo complejo, en el que coexisten normas constitucionales, legislación laboral, normativa de protección de datos además de la intensa labor interpretativa de los tribunales y otras autoridades de control. Lejos de ofrecer soluciones fijas, este marco impone una lógica de ponderación constante entre intereses legítimos (tales como seguridad, control organizativo, prevención de ilícitos) y derechos fundamentales cuya vigencia no se extingue por el mero hecho de acceder a un centro de trabajo o a un espacio vigilado.

2.4.1. Principios del tratamiento de datos aplicables

El primer límite jurídico a la videovigilancia viene determinado por la sujeción de las imágenes captadas al régimen general de protección de datos personales. La consideración de las imágenes como datos personales ha sido afirmada de forma reiterada tanto por el Tribunal Constitucional como por el Tribunal de Justicia de la Unión Europea, siempre que permitan identificar, directa o indirectamente, a las personas grabadas (STC 292/2000; TJUE, asunto C-212/13, Rynes¹⁵).

Entre los principios aplicables, el de licitud del tratamiento es uno de los más importantes. En el ámbito laboral y comercial, la base jurídica suele encontrarse en el interés legítimo del responsable, vinculado a la seguridad de personas y bienes o al ejercicio del poder de control empresarial, sin que resulte exigible, con carácter general, el consentimiento de los afectados (art. 6.1.f RGPD). No obstante, la doctrina ha insistido en que el recurso al interés legítimo no exonera de una ponderación rigurosa de los derechos en conflicto (Bygrave, 2014).

¹⁵ Tribunal de Justicia de la Unión Europea (Gran Sala), de 11 de diciembre de 2014, asunto C-212/13, *František Rynes contra Úřad pro ochranu osobních údajů*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62013CJ0212>

Otro principio relevante es el de proporcionalidad, entendido no como una fórmula retórica, sino como un canon material de control. La jurisprudencia constitucional ha subrayado que toda medida de vigilancia debe superar un triple juicio de idoneidad, necesidad y proporcionalidad en sentido estricto (STC 29/2013). En este contexto, la videovigilancia sólo resulta legítima cuando no existan medidas menos intrusivas igualmente eficaces para alcanzar la finalidad perseguida.

Asimismo, el principio de minimización de datos impone una restricción tanto en el alcance espacial como temporal de las grabaciones. La captación indiscriminada, continua o excesivamente amplia de imágenes ha sido considerada incompatible con la normativa de protección de datos, incluso cuando exista una finalidad legítima declarada (AEPD, 2025).

Por último, el principio de limitación de la finalidad obliga a que las imágenes se utilicen exclusivamente para los fines que justificaron su captación. La reutilización de grabaciones con objetivos distintos (por ejemplo, fines disciplinarios no previstos inicialmente o usos comerciales) ha sido objeto de especial reproche por parte de las autoridades de control y la doctrina especializada (Polo Roca, 2020).

2.4.2. Deberes del responsable del tratamiento

La licitud de la videovigilancia no depende únicamente de la finalidad perseguida, sino también del cumplimiento de una serie de deberes formales y materiales que recaen sobre el responsable del tratamiento. Entre ellos, el deber de información ocupa una posición especialmente relevante, al constituir una garantía básica para el ejercicio de los derechos de los afectados.

La normativa exige que los trabajadores y usuarios sean informados de manera previa, clara y accesible sobre la existencia de cámaras, su finalidad y la identidad del responsable del tratamiento (arts. 12 y 13 RGPD; art. 22 LOPDGDD). La jurisprudencia ha admitido fórmulas de información simplificada (como los distintivos visibles) siempre que permitan al interesado conocer la existencia del tratamiento y acceder fácilmente a información adicional (STC 39/2016¹⁶).

¹⁶ Tribunal Constitucional, STC 39/2016, de 3 de marzo.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2016-3405

Junto a ello, el responsable debe cumplir con las obligaciones de registro de actividades de tratamiento, documentando las características esenciales del sistema de videovigilancia. Esta exigencia, ligada al principio de responsabilidad proactiva, ha sido destacada por la doctrina como un elemento clave para garantizar la trazabilidad y el control ex post del tratamiento (Carazo Liébana, 2023).

En cuanto a la conservación de las imágenes, la normativa española ha establecido un plazo máximo general de un mes, salvo que deban conservarse para acreditar la comisión de actos ilícitos o para ponerlas a disposición de la autoridad competente (art. 22.3 LOPDGDD). La conservación indefinida o excesivamente prolongada ha sido considerada una infracción grave por la AEPD en numerosas resoluciones.

2.4.3. Obligaciones específicas del empresario y del titular del establecimiento

En el ámbito laboral, las obligaciones del responsable del tratamiento se ven reforzadas por la posición de superioridad jurídica del empresario respecto del trabajador. Esta asimetría justifica una interpretación particularmente exigente de los límites al control empresarial mediante videovigilancia.

El artículo 20.3 del Estatuto de los trabajadores reconoce al empresario facultades de vigilancia y control, pero la jurisprudencia ha reiterado que dichas facultades no son ilimitadas ni pueden ejercerse al margen de los derechos fundamentales (STC 186/2000). La doctrina laboralista ha insistido en que el poder de dirección debe ejercerse conforme a criterios de buena fe y respeto a la dignidad del trabajador (Baylos Grau, 2019).

En los establecimientos abiertos al público, el titular del local asume igualmente obligaciones específicas, especialmente en relación con la protección de los derechos de clientes y usuarios. La colocación de cámaras debe responder a riesgos reales y concretos, evitando configuraciones que supongan una vigilancia sistemática de zonas de tránsito general sin justificación suficiente (AEPD, 2025).

2.4.4. Derechos de los trabajadores y de los usuarios: información, acceso, oposición y tutela

Los sistemas de videovigilancia no pueden analizarse al margen de los derechos que asisten a las personas afectadas. El derecho de acceso a las imágenes, el derecho de

oposición y el derecho a la tutela efectiva ante autoridades administrativas y judiciales constituyen contrapesos esenciales frente a posibles abusos.

La experiencia práctica demuestra, sin embargo, que el ejercicio efectivo de estos derechos se ve dificultado por la falta de información y por la brevedad de los plazos de conservación. La doctrina ha señalado que esta debilidad estructural refuerza la necesidad de controles preventivos y de una interpretación garantista de las obligaciones del responsable (Garriga Domínguez, 2009).

2.4.5. Espacios especialmente protegidos: vestuarios, aseos, zonas de descanso

Existe un consenso normativo y jurisprudencial claro en torno a la prohibición casi absoluta de instalar cámaras en determinados espacios considerados especialmente sensibles. Vestuarios, aseos y zonas de descanso forman parte del núcleo más intenso de la intimidad, incluso dentro del ámbito laboral.

La instalación de cámaras en estos espacios ha sido considerada, de forma reiterada, una vulneración directa del artículo 18 CE, sin que pueda justificarse por razones organizativas o de seguridad ordinaria. La doctrina coincide en que se trata de un límite infranqueable, salvo supuestos excepcionales extremadamente cualificados (Pérez Luño, 1999).

2.4.6. La grabación sonora, la videovigilancia encubierta y el uso de tecnologías avanzadas

La grabación de sonido, la videovigilancia encubierta y el uso de tecnologías avanzadas como la inteligencia artificial o la biometría representan los supuestos de mayor intensidad lesiva para los derechos fundamentales.

La grabación de audio mediante sistemas de videovigilancia constituye, con carácter general, un tratamiento desproporcionado e intrusivo. El artículo 89.3 de la LOPDGDD solo admite la grabación de sonidos en el lugar de trabajo cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad desarrollada, y siempre debidamente justificados respetando el principio de proporcionalidad, dada su especial capacidad de invasión a la intimidad.

En este sentido, la doctrina del TC (STC 98/2000) señala que la grabación de conversaciones entre trabajadores o entre éstos y los clientes, no puede justificarse únicamente por el interés empresarial de controlar el cumplimiento de las obligaciones laborales, al afectar directamente al derecho fundamental al secreto de las comunicaciones reconocido en el artículo 18.3 CE. No obstante, ello no implica una prohibición absoluta, sino que la doctrina admite su posible legitimidad en supuestos excepcionales, siempre que concurran circunstancias especialmente cualificadas, como la existencia de sospechas graves de conductas ilícitas, la relevancia del bien jurídico protegido y la inexistencia de medidas menos intrusivas. En estos casos, la medida deberá superar un juicio estricto de proporcionalidad y contar con garantías reforzadas.

Esta cuestión ha generado una intensa polémica doctrinal, ya que parte de la doctrina considera que la grabación de comunicaciones constituye una injerencia especialmente intensa en los derechos fundamentales, difícilmente compatible con el ámbito laboral, mientras que otros sectores admiten su utilización en contextos muy delimitados, especialmente cuando se trata de prevenir o acreditar conductas ilícitas de especial gravedad.

La videovigilancia encubierta se define como aquella que implica la ocultación deliberada de los sistemas de grabación respecto de las personas afectadas, careciendo de información previa sobre su instalación. Su utilización debe interpretarse de manera restrictiva y excepcional. En particular, la jurisprudencia del TEDH, en el asunto *López Ribalda y otros contra España* (17 de octubre de 2019), ha considerado que este tipo de medidas puede resultar legítimo cuando concurren sospechas graves y fundadas de conductas ilícitas, no existen medidas menos intrusivas igualmente eficaces, y la vigilancia se limita espacial y temporalmente a lo estrictamente necesario para la finalidad perseguida. Asimismo, se exige que la medida respete el principio de proporcionalidad y que existan garantías suficientes frente a posibles abusos.

El uso de tecnologías avanzadas, como la inteligencia artificial aplicada a sistemas de videovigilancia, no se limita únicamente al tratamiento de datos biométricos, sino que incluye también herramientas de análisis automatizado de comportamiento, detección de anomalías, reconocimiento de patrones o evaluación del rendimiento laboral. Estas tecnologías permiten, por ejemplo, monitorizar tiempos de actividad, identificar conductas consideradas inusuales o generar perfiles de comportamiento a partir de datos agregados, lo que incrementa significativamente la capacidad de control empresarial.

Este tipo de sistemas plantea importantes riesgos desde la perspectiva de los derechos fundamentales, especialmente en relación con la privacidad, la autonomía personal y la no discriminación, al introducir mecanismos de vigilancia permanente y decisiones automatizadas que pueden afectar a los trabajadores sin intervención humana directa.

En este contexto, cobra especial relevancia el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, conocido como Reglamento de Inteligencia Artificial de la Unión Europea, que establece un enfoque basado en el riesgo y clasifica determinados usos de la inteligencia artificial como de “alto riesgo”, incluyendo aquellos destinados a la gestión y control de trabajadores. Este Reglamento impone obligaciones estrictas en materia de transparencia, supervisión humana, calidad de los datos y evaluación de impacto, y prohíbe determinadas prácticas, como el uso de sistemas de reconocimiento de emociones en el ámbito laboral o la clasificación de personas en función de características sensibles.

Asimismo, el RGPD refuerza la necesidad de que estos sistemas respeten los principios de minimización de datos, limitación de la finalidad y proporcionalidad, evitando el uso indiscriminado de tecnologías que puedan derivar en formas de vigilancia masiva o en decisiones automatizadas carentes de garantías suficientes.

2.5. Análisis jurisprudencial y doctrinal

La construcción jurídica de los límites a la videovigilancia en el ámbito laboral y comercial no ha sido el resultado de una regulación cerrada y exhaustiva, sino de un proceso progresivo de interpretación jurisprudencial en el que los tribunales han desempeñado un papel decisivo. En este proceso, la videovigilancia se ha convertido en un terreno en el que conciliar derechos fundamentales y poderes de control, especialmente en contextos marcados por relaciones de desigualdad estructural, como la relación laboral.

2.5.1. Jurisprudencia del Tribunal Constitucional en materia de videovigilancia laboral

El TC ha sido el primer actor en establecer unos criterios esenciales en la materia. Desde sus primeras resoluciones, el Tribunal ha señalado que la existencia de una relación de trabajo no supone una renuncia a los derechos fundamentales del trabajador, sino

únicamente una modulación en su ejercicio compatible con las exigencias de la organización productiva (STC 98/2000; STC 186/2000). Esta afirmación, que hoy nos parece obvia, resultó clave para frenar concepciones expansivas del poder empresarial que pretendían justificar controles intensivos al amparo del contrato de trabajo.

La doctrina constitucional ha insistido de forma reiterada en la necesidad de aplicar el juicio de proporcionalidad a cualquier medida de vigilancia. Así, en la STC 29/2013, el Tribunal establece con claridad que la idoneidad de la medida no basta por sí sola para legitimar la videovigilancia, siendo imprescindible comprobar si resulta necesaria y si el sacrificio del derecho fundamental no es excesivo en relación con el beneficio perseguido. Esta lógica de ponderación ha sido especialmente relevante en supuestos de captación continua de imágenes o de vigilancia generalizada de la actividad laboral.

Un punto de inflexión en la jurisprudencia constitucional lo constituye la STC 39/2016, en la que el Tribunal admite la validez probatoria de imágenes captadas mediante videovigilancia visible, aun cuando la información proporcionada a los trabajadores fuera genérica. El TC fundamenta su decisión en que el trabajador tenía conocimiento de la existencia del sistema de videovigilancia en el centro de trabajo, lo que considera suficiente para entender cumplido el deber de información, en relación con la finalidad legítima de control laboral reconocida al empresario. Asimismo, el Tribunal entiende que la medida supera el juicio de proporcionalidad, al resultar idónea y necesaria para la detección de irregularidades.

No obstante, la sentencia ha generado un intenso debate doctrinal, al entender algunos autores que el Tribunal flexibiliza en exceso el deber de información, desplazando el centro de gravedad hacia la eficacia del control empresarial (Baylos Grau, 2019), mientras que otros consideran que se trata de una adaptación razonable a la realidad de los sistemas de seguridad en entornos laborales complejos (Garriga Domínguez, 2009). La resolución cuenta, además, con votos particulares en los que se cuestiona la suficiencia de la información facilitada al trabajador, advirtiendo del riesgo de vaciar de contenido las garantías del derecho fundamental a la protección de datos si se admiten formas de información excesivamente genéricas.

2.5.2. Doctrina del Tribunal Supremo

El TS, por su parte, ha desarrollado una jurisprudencia continuista, aunque con matices, centrada en la utilización de las grabaciones como medio de prueba en procedimientos disciplinarios. De forma reiterada, ha declarado lícita la utilización de imágenes cuando la instalación de cámaras responde a finalidades de seguridad o control legítimas y cuando los trabajadores han sido informados de su existencia, aunque sea de manera genérica (STS de 26 de septiembre de 2007¹⁷; STS 77/2017¹⁸). No obstante, el alto tribunal ha mostrado una mayor cautela en los supuestos de videovigilancia encubierta, subrayando su carácter excepcional y la necesidad de que concurren sospechas fundadas de conductas ilícitas graves.

2.5.3. Jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) (*especial referencia al caso López Ribalda y otros contra España 2019*)

La dimensión europea del problema ha adquirido una relevancia decisiva a raíz de la jurisprudencia del TEDH, especialmente con el conocido caso *López Ribalda y otros c. España 2019*. En su primera sentencia de 2018, el TEDH consideró que la instalación de cámaras ocultas sin información previa, vulneraba el artículo 8 del Convenio Europeo de Derechos Humanos. Sin embargo, la sentencia de la Gran Sala de 2019 matizó esta posición, admitiendo la licitud de la videovigilancia encubierta en circunstancias excepcionales, cuando existan sospechas razonables de irregularidades graves, la medida sea limitada en el tiempo, y el acceso a las grabaciones esté estrictamente controlado.

Esta segunda sentencia ha sido objeto de una abundante discusión doctrinal. Algunos autores han advertido del riesgo de que la excepción termine convirtiéndose en regla, debilitando las garantías del derecho a la vida privada en el ámbito laboral (Rodríguez de Santiago, 2019). Otros, en cambio, subrayan que el TEDH no legitima una vigilancia indiscriminada, sino que refuerza la necesidad de un análisis contextualizado y restrictivo de cada caso concreto (De Hert y Papakonstantinou, 2016).

¹⁷ Tribunal Supremo, Sala de lo Social, STS de 26 de septiembre de 2007, rec. 966/2006. <https://vlex.es/vid/on-i-re-31962968>

¹⁸ Tribunal Supremo, Sala de lo Social, STS 77/2017, de 31 de enero. <https://vlex.es/vid/670490065>

2.5.4. Resoluciones relevantes de la Agencia Española de Protección de Datos

Junto a los tribunales, la AEPD ha desempeñado un papel fundamental en la concreción práctica de los límites jurídicos a la videovigilancia. A través de resoluciones sancionadoras, informes y guías interpretativas, la AEPD ha contribuido a delimitar cuestiones como la conservación de imágenes, la prohibición de grabar sonido o la instalación de cámaras en espacios especialmente protegidos. En el ámbito comercial, son especialmente relevantes las resoluciones que sancionan la captación de la vía pública sin justificación suficiente, o la conservación prolongada de grabaciones sin causa legítima, reforzando una interpretación estricta de los principios de minimización y proporcionalidad.

2.5.5. Casos prácticos: centros de trabajo, comercios y comunidades de propietarios

Los conflictos relacionados con la videovigilancia suelen aparecer en distintos ámbitos, como los centros de trabajo, los establecimientos comerciales o las comunidades de propietarios. Estos espacios presentan características jurídicas y funcionales diferentes.

En el ámbito laboral, la videovigilancia suele vincularse al control de la actividad profesional y a la seguridad de las instalaciones, lo que introduce el debate sobre los límites del poder de dirección del empresario y el respeto a la intimidad de los trabajadores. En los establecimientos comerciales, en cambio, la videovigilancia se orienta principalmente a la prevención de hurtos y a la protección de bienes y personas. Por su parte, en las comunidades de propietarios la videovigilancia se orienta, con carácter general, a la protección de los espacios comunes y a la mejora de la seguridad de los residentes.

2.5.6. Convergencias y divergencias en la doctrina de los tribunales

En consecuencia, el análisis jurídico de la videovigilancia debe realizarse atendiendo al contexto concreto en el que se utiliza. Por ello, tanto los tribunales como las autoridades de control valoran no solo la finalidad declarada del sistema, sino también su

configuración técnica, el alcance real de la captación de imágenes y el impacto que puede tener sobre los derechos de las personas afectadas.

La experiencia acumulada muestra que las soluciones maximalistas (ya sea en favor de la seguridad o de la privacidad) resultan insatisfactorias, imponiéndose una lógica de equilibrio dinámico y casuístico.

En general, la jurisprudencia y la doctrina coinciden en que la videovigilancia no es en sí misma incompatible con los derechos fundamentales, pero sí potencialmente lesiva cuando se utiliza de forma intensiva, opaca o desproporcionada. El verdadero desafío jurídico no reside tanto en la admisibilidad abstracta de estas tecnologías como en la construcción de límites efectivos que eviten su normalización acrítica, y preserven espacios reales de libertad personal en entornos cada vez más vigilados.



3. Propuesta de modelo de videovigilancia respetuoso con la privacidad en el ámbito laboral y comercial

El análisis jurídico y jurisprudencial que hemos realizado a lo largo de estas páginas nos permite afirmar que la videovigilancia no es contraria al ordenamiento jurídico, pero sí es un recurso potencialmente lesivo de derechos fundamentales cuando se diseña o aplica sin criterios estrictos de necesidad y proporcionalidad. Es decir, la mayor parte de los conflictos no tienen que ver con la finalidad declarada, que suele ser legítima, sino con su configuración técnica, con su extensión espacial o temporal o con la ausencia de garantías efectivas para trabajadores y usuarios. Por ello nuestra propuesta se basa en un sistema de videovigilancia para que su diseño incluya, desde el principio, la protección de la privacidad como elemento estructural y no como algo formal.

El modelo que proponemos se basa en la sistematización de los principios establecidos en el RGPD, la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, la jurisprudencia constitucional y europea, así como en los criterios interpretativos de la AEPD y del Comité Europeo de Protección de Datos.

En este sentido, no se configura como un protocolo normativo autónomo, sino como una propuesta de sistematización operativa y como una guía de buenas prácticas orientada a traducir las exigencias jurídicas en un modelo estructurado en siete pilares aplicables al diseño, implantación y supervisión de sistemas de videovigilancia. Se trata de una sistematización operativa, en consecuencia, de las exigencias que presenta la normativa actual y la doctrina.

PASO 1: Evaluación de necesidad

Antes de instalar cualquier sistema de videovigilancia, debe realizarse una evaluación documentada de necesidad y proporcionalidad, que incluya (I) la identificación concreta del riesgo que se pretende prevenir, (II) la justificación de la insuficiencia de medidas menos intrusivas, (III) la delimitación exacta del espacio y el tiempo de grabación y (IV) la evaluación del impacto sobre derechos fundamentales, en línea con los principios de licitud, minimización y responsabilidad proactiva recogidos en los artículos 5 y 24 del RGPD.

En supuestos de especial intensidad (vigilancia sistemática de trabajadores, uso de tecnologías avanzadas, captación en espacios sensibles), debería realizarse una evaluación de impacto en protección de datos, tal y como se recoge en el artículo 35 del RGPD.

Este requisito responde además al principio de proporcionalidad desarrollado por el TC, que exige superar los juicios de idoneidad, necesidad y proporcionalidad en sentido estricto (STC 29/2013). Por eso incluimos este primer paso en nuestro proyecto como algo indispensable.

PASO 2: Delimitación de la finalidad

El sistema debe configurarse con finalidades determinadas, explícitas y legítimas, conforme al principio de limitación de la finalidad (art. 5.1.b RGPD) diferenciando claramente entre (I) seguridad de personas y bienes, (II) prevención de ilícitos concretos y, (III) control de cumplimiento laboral en los términos del artículo 20.3 del Estatuto de los Trabajadores. Es decir, no se pueden admitir finalidades genéricas o abiertas tales como “mejorar el rendimiento”, “optimizar la productividad”, si eso supone vigilar intensamente al trabajador.

Además, las imágenes no podrán reutilizarse para fines distintos de los declarados y cualquier cambio de finalidad exigirá un nuevo estudio de proporcionalidad.

Este paso es fundamental para evitar la expansión funcional de la vigilancia, que es uno de los principales riesgos en los que suele caerse.

PASO 3: Diseño técnico orientado a la minimización

El modelo propone incorporar la minimización (artículo 5.1.C RGPD) no solo como principio jurídico, sino como criterio técnico de configuración del sistema:

- Limitación espacial: es decir, cámaras exclusivamente en zonas de riesgo real, prohibición absoluta en vestuarios, aseos o zonas de descanso y, evitar la captación innecesaria de vía pública o espacios colindantes.
- Limitación temporal: grabación preferentemente continua solo cuando esté justificada, valoración de sistemas activados por eventos y conservación máxima general de 30 días (art. 22 de la LOPDGDD) con supresión automática.

- Limitación funcional: es decir, prohibir en general la grabación de sonido, prohibir el análisis automatizado de comportamiento sin evaluación específica y prohibir los sistemas de reconocimiento facial en el ámbito laboral ordinario.

El sistema debe configurarse técnicamente para impedir usos abusivos, y no limitarse a confiar en la buena fe de la persona responsable.

PASO 4: Transparencia reforzada y derecho a la información efectiva

La transparencia constituye una garantía esencial del tratamiento de datos (arts. 12 y 13 RGPD), especialmente en el ámbito laboral, donde existe una evidente asimetría entre las partes.

Para que dicha información sea comprensible, efectiva, y no meramente formal, el modelo propone un sistema de información por capas, conforme a las recomendaciones de la AEPD:

Primera capa (información básica *in situ*): mediante carteles visibles situados en las zonas videovigiladas, que indiquen al menos la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercer derechos.

Segunda capa (información ampliada): accesible a través de documentos internos, intranet, página web o códigos QR, donde se detalle la finalidad concreta del sistema, base jurídica, plazos de conservación y vías de ejercicio de derechos.

En el ámbito laboral, esta información deberá complementarse con la comunicación previa a los trabajadores o sus representantes, de conformidad con la normativa laboral aplicable.

Asimismo, se propone incorporar medidas adicionales de refuerzo, tales como: Entrega de cláusulas informativas específicas en el momento de la contratación, inclusión de la política de videovigilancia en los protocolos internos de la empresa y realización de acciones informativas o formativas cuando se implanten sistemas especialmente intrusivos.

De este modo, la transparencia se configura como un mecanismo real de control por parte de los afectados, evitando que la información quede reducida a un cumplimiento meramente formal.

La videovigilancia encubierta únicamente sería admisible en supuestos excepcionales, conforme a los criterios establecidos por el TEDH.

PASO 5: Gobernanza interna y responsabilidad proactiva

El modelo debe incorporar mecanismos organizativos orientados al cumplimiento del principio de responsabilidad proactiva conforme al artículo 24 RGPD que refuercen el control interno, es decir, un registro detallado del sistema de videovigilancia, el control de acceso a las grabaciones, un protocolo interno de uso disciplinario y auditorías periódicas del sistema.

La responsabilidad proactiva implica que el empresario o titular del establecimiento pueda acreditar en todo momento la licitud y proporcionalidad del sistema.

PASO 6: Refuerzo de derechos de trabajadores y usuarios

En línea con los derechos reconocidos en los artículos 15 y siguientes del RGPD, el modelo prevé la implantación de un procedimiento¹⁹ accesible y claro para el ejercicio del derecho de acceso, que permita a los interesados conocer si están siendo objeto de grabación y, en su caso, acceder a las imágenes en las que aparezcan, en los términos legalmente previstos.

Asimismo, se establece la obligación de emitir una respuesta motivada en caso de denegación, especialmente cuando concurran límites derivados de la protección de derechos de terceros o de la seguridad pública.

Cuando las grabaciones se utilicen con fines disciplinarios, deberá garantizarse al trabajador el conocimiento efectivo del contenido y alcance de las imágenes utilizadas, en coherencia con el derecho de defensa.

¹⁹ El procedimiento deberá incluir, al menos: (I) la identificación del solicitante, (II) la especificación aproximada de la fecha, franja horaria y lugar de la grabación, (III) la verificación de la identidad del interesado, (IV) el análisis de la posible afectación a derechos de terceros, (V) la visualización de las imágenes en condiciones controladas o, en su caso, la entrega de copia anonimizada, y (VI) la resolución en el plazo máximo de un mes conforme al artículo 12 del RGPD.

PASO 7: Cultura organizativa de respeto a la privacidad

El modelo propone incorporar una dimensión ética basada en el principio de protección de datos desde el diseño y por defecto según el artículo 25 del RGPD, por lo que se deberá integrar la privacidad como valor corporativo y evitar la normalización de la vigilancia permanente.

Además, se deberá evaluar periódicamente si el sistema sigue siendo necesario y también se revisará la proporcionalidad en función de la evolución del riesgo. En definitiva, la seguridad no puede convertirse en un argumento expansivo ilimitado, sino que debe operar como instrumento al servicio de los derechos fundamentales, no como algo que los erosione.

En conclusión, un modelo de videovigilancia respetuoso con la privacidad debe seguir estos siete pasos, pues a partir de ellos el modelo no impide la seguridad ni el control empresarial, pero sí transforma su lógica. Es decir, la vigilancia deja de ser una herramienta de supervisión expansiva para convertirse en una medida excepcional, delimitada y sujeta a responsabilidad jurídica.

Como se ha expuesto a lo largo de este epígrafe, en un contexto de creciente digitalización e innovación tecnológica, la protección de la privacidad no puede descansar únicamente en la reacción judicial posterior, sino que debe incorporarse estructuralmente al diseño de los sistemas de control. Para ello, además de reforzar las garantías jurídicas existentes, resulta igualmente necesario potenciar la información, la formación y la concienciación sobre el uso adecuado de los sistemas de videovigilancia y sobre los límites que derivan de la protección de los derechos fundamentales. Solo desde una combinación de regulación, supervisión y cultura de respeto a la privacidad puede mantenerse un equilibrio real entre seguridad y derechos fundamentales.

4. Resultados

El análisis normativo, jurisprudencial y doctrinal desarrollado a lo largo de este trabajo nos permite extraer una serie de resultados que reflejan tendencias claras y conclusiones bastante relevantes sobre el estado actual del equilibrio entre seguridad y derecho a la intimidad en el ámbito laboral y comercial.

En primer lugar, puede afirmarse que el ordenamiento jurídico español y europeo dispone de un marco normativo suficientemente garantista para proteger el derecho a la privacidad frente a los riesgos derivados de la videovigilancia. La Constitución Española, en su artículo 18, insiste tanto en la protección de la intimidad como en el derecho fundamental a la protección de datos, en este último caso a través de la configuración jurisprudencial. A ello se suma el desarrollo legislativo recogido en el RGPDD, el Reglamento General de la IA de Europa, y la Ley Orgánica 3/2018, que incorporan principios claros como la minimización, la limitación de la finalidad o la responsabilidad proactiva.

Tal y como hemos visto, el problema no radica tanto en la ausencia de normas como en la forma en que estas se aplican y se concretan en la práctica. De hecho, el análisis de la jurisprudencia revela que los conflictos no suelen producirse por la mera existencia de cámaras, sino por su configuración excesiva, por la falta de información adecuada o por la utilización posterior de las grabaciones con fines distintos de los inicialmente declarados. El derecho positivo ofrece herramientas suficientes para evitar abusos, pero su efectividad depende casi siempre de la interpretación judicial y del compromiso real de los responsables del tratamiento.

Otro resultado observado en estas páginas es la consolidación del principio de proporcionalidad como eje vertebrador del control constitucional de la videovigilancia. La jurisprudencia del TC ha reiterado que cualquier medida restrictiva de derechos fundamentales debe superar los juicios de idoneidad, necesidad y proporcionalidad en sentido estricto. Este argumento se ha convertido en el criterio decisivo para evaluar la legitimidad de los sistemas de vigilancia, desplazando concepciones más formales o basadas exclusivamente en la titularidad del poder empresarial.

Sin embargo, el análisis también muestra que la aplicación concreta del juicio de proporcionalidad no siempre es homogénea. En algunos supuestos, especialmente cuando concurren cuestiones de seguridad o prevención de ilícitos, los tribunales han adoptado

una interpretación más flexible, admitiendo sistemas de control amplios siempre que exista una justificación razonable. Esta tendencia se aprecia sobre todo en el ámbito laboral, donde el poder de dirección del empresario reconocido en el artículo 20.3 del Estatuto de los Trabajadores introduce un elemento de complejidad adicional.

Respecto a la jurisprudencia europea, el caso *López Ribalda* constituye, sin duda, un punto de inflexión. El análisis de esta sentencia y de su evolución nos permite apreciar un pequeño conflicto entre la exigencia de información previa y la admisión excepcional de videovigilancia encubierta. El TEDH no legitima la vigilancia oculta como práctica ordinaria, pero sí admite su utilización en circunstancias concretas, cuando existan sospechas graves y la medida esté limitada en el tiempo y en su alcance.

Por lo tanto, de la evolución de la jurisprudencia podemos extraer dos conclusiones. Por un lado, se reafirma la importancia de la transparencia como regla general, y por otro, se abre un margen de excepcionalidad que, si no se interpreta de forma restrictiva, podría erosionar progresivamente las garantías del derecho a la vida privada en el ámbito laboral. La clave parece estar en evitar que la excepción se normalice.

También creo que es importante hablar de la especial vulnerabilidad de la persona trabajadora dentro del esquema de videovigilancia. Aunque la doctrina constitucional ha insistido en que el contrato de trabajo no implica renuncia a los derechos fundamentales, la realidad de la relación laboral genera bastante asimetría. El trabajador no se encuentra en una posición de igualdad respecto de la persona empresaria a la hora de cuestionar la instalación o el funcionamiento de sistemas de control. Esta asimetría justifica una interpretación especialmente cuidadosa de las medidas de vigilancia en el entorno laboral. El uso disciplinario de grabaciones constituye el foco principal de conflictos y evidencia la necesidad de establecer límites claros en cuanto al acceso, conservación y utilización probatoria de las imágenes. El análisis realizado en este trabajo confirma que cuando estas garantías no están claramente delimitadas, el riesgo de vulneración de derechos aumenta considerablemente.

En el ámbito comercial, el resultado más significativo es apreciar una progresiva normalización de la videovigilancia. La presencia de cámaras en establecimientos abiertos al público se ha convertido en un elemento habitual en las ciudades, lo que ha contribuido a reducir la percepción social de intromisión. Sin embargo, el hecho de que la expectativa de privacidad sea menor en estos espacios no implica su desaparición. La captación sistemática de imágenes de clientes sigue constituyendo un tratamiento de datos

personales sujeto a límites estrictos. Como hemos visto, parece que el riesgo actual no reside únicamente en la cámara como dispositivo aislado, sino en su integración con tecnologías avanzadas de análisis automatizado. La posibilidad de incorporar inteligencia artificial, reconocimiento facial o sistemas de perfilado comportamental transforma todavía más el alcance de la videovigilancia. Aunque estas tecnologías no estén generalizadas en todos los contextos laborales y comerciales, su mera disponibilidad tecnológica obliga a replantear los estándares de protección.

En este sentido, uno de los resultados más importantes del trabajo es apreciar un desplazamiento progresivo desde una vigilancia reactiva hacia una vigilancia preventiva y, en algunos casos, predictiva. La lógica preventiva, orientada a detectar irregularidades antes de que se produzcan daños, podría ser eficaz desde el punto de vista organizativo, pero plantea interrogantes profundos desde la perspectiva de los derechos fundamentales. Cuando la vigilancia deja de responder a riesgos concretos y se convierte en un mecanismo permanente de supervisión generalizada, el equilibrio entre seguridad y privacidad se inclina peligrosamente hacia el control. En definitiva, la tensión entre seguridad y derecho a la intimidad no es coyuntural ni circunstancial, sino estructural. Ambas dimensiones responden a valores constitucionales legítimos y necesarios. La seguridad protege bienes jurídicos relevantes y facilita la convivencia social; la privacidad garantiza la autonomía personal y la dignidad. El desafío jurídico consiste en articular mecanismos que impidan que uno de estos valores absorba al otro.

Tampoco podemos olvidarnos de la importancia creciente del principio de responsabilidad proactiva. El RGPD ha desplazado el centro de gravedad desde el cumplimiento formal hacia la obligación de demostrar activamente la conformidad del tratamiento con la normativa. Esta exigencia adquiere especial relevancia en materia de videovigilancia, donde la intensidad potencial de la injerencia requiere una justificación documentada y verificable. El modelo que hemos propuesto en el epígrafe anterior va en esa línea preventiva.

En definitiva, se observa que la cuestión de la videovigilancia no puede abordarse exclusivamente desde parámetros técnicos o económicos. La forma en que se diseñan y aplican estos sistemas refleja una determinada concepción del espacio laboral y comercial. Si se conciben como entornos de confianza regulada, la vigilancia tenderá a ser limitada y contextualizada. Si, por el contrario, se perciben como espacios de sospecha permanente, la expansión del control resultará casi inevitable. El ordenamiento jurídico

ofrece herramientas suficientes para proteger la privacidad frente a la videovigilancia, pero también evidencian la fragilidad del equilibrio cuando la aplicación práctica se aleja de los principios de proporcionalidad, transparencia y minimización. El desafío actual no consiste en prohibir la tecnología, sino en someterla de manera efectiva a los valores constitucionales que estructuran el Estado social y democrático de derecho.



5. Conclusiones

Del análisis realizado a lo largo de este trabajo pueden extraerse las siguientes conclusiones:

Primera. La videovigilancia en el ámbito laboral y en los establecimientos abiertos al público constituye uno de los escenarios que mejor refleja la tensión contemporánea entre seguridad y derechos fundamentales. No se trata de un conflicto puntual ni de un problema exclusivamente técnico, sino de un fenómeno estructural que evidencia cómo las sociedades democráticas gestionan el equilibrio entre control y libertad en un contexto crecientemente digitalizado.

Segunda. El ordenamiento jurídico español y europeo dispone de un marco normativo sólido para la protección de la privacidad y de los datos personales. El artículo 18 CE, junto con el desarrollo legislativo en materia de protección de datos y la influencia decisiva del RGPD, configuran un sistema garantista en abstracto. La jurisprudencia del TC, del TS y del TEDH ha contribuido a perfilar criterios relativamente estables en torno a la proporcionalidad, la información previa y el carácter excepcional de la videovigilancia encubierta. Sin embargo, este marco normativo no acaba con la tensión. El problema no radica en la inexistencia de límites, sino en su aplicación práctica y en la evolución tecnológica constante que amplía las capacidades de control. La facilidad técnica para captar, almacenar y analizar imágenes convierte la videovigilancia en una herramienta cada vez más accesible y sofisticada, lo que exige una interpretación dinámica y exigente de los principios constitucionales.

Tercera. El ámbito laboral es un escenario complejo para este debate. Aunque el poder de dirección y control del empresario está reconocido legalmente, la relación laboral se caracteriza por una asimetría que intensifica el riesgo de vulneración de derechos fundamentales. Ni el trabajador pierde su condición de titular de derechos por el hecho de integrarse en una organización productiva, ni la dignidad y la autonomía personal se suspenden durante la jornada laboral. En este contexto, la videovigilancia puede cumplir funciones legítimas de seguridad y control, pero su diseño y aplicación deben someterse a un control muy riguroso. El uso disciplinario de grabaciones, la ausencia de información clara o la instalación de sistemas técnicamente desproporcionados constituyen los principales focos de conflicto.

Cuarta. En el ámbito comercial, aunque la expectativa de privacidad sea menor, no desaparece del todo. La normalización social de la presencia de cámaras no debe interpretarse como una aceptación sin más de cualquier forma de vigilancia. La captación sistemática de imágenes en establecimientos abiertos al público sigue siendo un tratamiento de datos personales que exige justificación, minimización y transparencia. La protección de los clientes y usuarios no puede quedar relegada a un segundo plano bajo el argumento genérico de la seguridad.

Quinta. La evolución tecnológica ha transformado cualitativamente el alcance de la videovigilancia. La integración de inteligencia artificial, reconocimiento facial y sistemas de análisis automatizado no solo permite registrar hechos pasados, sino detectar patrones, clasificar comportamientos e incluso anticipar riesgos. Esta transformación introduce un cambio profundo en la naturaleza del control y plantea interrogantes que el marco normativo tradicional debe abordar con cautela. En realidad, el riesgo actual no reside tanto en la cámara aislada como en el diseño digital que puede construirse en torno a ella. En este sentido, puede afirmarse que, si bien se han producido avances normativos relevantes, la regulación, y especialmente su aplicación práctica, no evolucionan al mismo ritmo que el desarrollo tecnológico. Esta asimetría genera espacios de incertidumbre y riesgo para los derechos fundamentales. En consecuencia, si no se consolidan y aplican de forma efectiva unos límites claros, la videovigilancia podría evolucionar hacia formas de supervisión permanente difíciles de percibir y aún más difíciles de cuestionar. La protección de la privacidad exige anticiparse a estos escenarios y reforzar la exigencia de evaluaciones de impacto, prohibiciones específicas y restricciones a las decisiones automatizadas.

Sexta. La seguridad y la privacidad no son valores incompatibles, pero sí enfrentados constantemente. La seguridad cumple una función instrumental esencial en el Estado de derecho: protege bienes jurídicos y garantiza condiciones mínimas de convivencia. Sin embargo, cuando se lleva a cabo de manera expansiva y sin delimitación concreta, puede convertirse en un argumento capaz de justificar restricciones desproporcionadas de derechos fundamentales.

Séptima. El equilibrio no se alcanza prohibiendo de forma absoluta la videovigilancia y tampoco aceptándose sin reservas, sino mediante una regulación cuidadosa, contextualizada y sometida a revisión constante. La proporcionalidad no es una fórmula retórica, sino un método de análisis que exige examinar cada sistema en función de su

finalidad, alcance y efectos reales. La propuesta de modelo desarrollada en este trabajo responde precisamente a esa necesidad de concretar el equilibrio en términos operativos. No se limita a reiterar principios generales, sino que plantea una estructura de prevención basada en la evaluación previa de necesidad, la delimitación estricta de finalidades, la minimización técnica, la transparencia reforzada y la responsabilidad proactiva. El objetivo no es obstaculizar la seguridad, sino integrarla en un marco coherente con los valores constitucionales.

Octava. La cuestión de la videovigilancia remite a una reflexión más profunda sobre el tipo de entorno laboral y comercial que se desea construir. Un espacio caracterizado por la confianza regulada y el respeto a la autonomía personal es compatible con medidas de control limitadas y justificadas. Sin embargo, un modelo basado en la sospecha permanente tiende a expandir progresivamente la vigilancia, reduciendo el margen de libertad individual. Esta evolución plantea además una cuestión de especial relevancia: si la progresiva normalización de mecanismos de control inicialmente excepcionales está alterando paulatinamente la percepción social de la privacidad. Existe el riesgo de que ésta deje de concebirse como un ámbito inherente a la persona merecedor de protección para pasar a entenderse como una realidad disponible o subordinada a intereses de control, eficiencia u organización. Hay que entender que la protección de la privacidad no constituye un obstáculo para la eficacia organizativa, sino una condición para preservar la legitimidad del ejercicio del poder en contextos privados. En un Estado social y democrático de derecho, la empresa y los establecimientos comerciales no son espacios exentos de control constitucional. Los derechos fundamentales acompañan a las personas en todos los ámbitos en los que desarrollan su vida.

Novena. En definitiva, el equilibrio entre seguridad y derecho a la intimidad en la videovigilancia laboral y comercial no constituye un debate cerrado, sino un proceso dinámico que exige vigilancia jurídica constante. El reto principal no consiste en frenar la tecnología, sino en gobernarla conforme a los principios constitucionales, evitando que la búsqueda de seguridad termine erosionando silenciosamente los espacios de libertad que pretende proteger.

En este sentido, el problema no radica en la existencia de sistemas de videovigilancia o mecanismos tecnológicos de control, sino en la forma en que estos son utilizados y en los límites que deben respetarse durante su aplicación. La evolución tecnológica ha permitido desarrollar herramientas cada vez más eficaces para la prevención de riesgos y

la mejora de la seguridad, aunque dicha evolución también exige reforzar las garantías destinadas a proteger los derechos fundamentales de las personas. Por ello, resulta necesario avanzar hacia modelos de utilización basados en criterios de proporcionalidad, transparencia y mínima injerencia, especialmente en aquellos ámbitos donde la vigilancia pueda afectar de manera directa a la intimidad o a la libertad individual.

Del mismo modo, sería conveniente que futuras reformas legislativas concretasen con mayor precisión los límites aplicables al uso de tecnologías avanzadas de vigilancia, particularmente aquellas basadas en inteligencia artificial, reconocimiento biométrico o sistemas automatizados de análisis de comportamiento. La ausencia de una regulación más específica en determinados aspectos puede generar situaciones de inseguridad jurídica y riesgos de utilización desproporcionada, por lo que se considera necesario establecer mecanismos de control y supervisión adecuados que garanticen un equilibrio real entre las necesidades de seguridad y la protección de los derechos fundamentales.

Finalmente, la protección efectiva de la privacidad en entornos cada vez más digitalizados no puede depender exclusivamente de mecanismos normativos o de control judicial posterior. Resulta igualmente necesario fomentar una mayor formación y capacitación digital de ciudadanos, trabajadores y usuarios, permitiéndoles comprender de manera más clara el funcionamiento de los sistemas de videovigilancia, el alcance del tratamiento de sus datos personales y los derechos que les asisten frente a posibles usos abusivos o desproporcionados. La protección de los derechos fundamentales exige hoy no solo garantías jurídicas, sino también una ciudadanía digital consciente e informada.

A) NORMATIVA, DOCUMENTACIÓN Y JURISPRUDENCIA

Normativa europea

- ❖ Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- ❖ 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, por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- ❖ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y se modifican determinados actos legislativos de la Unión (Reglamento de Inteligencia Artificial).

Normativa española

- ❖ Constitución Española, de 27 de diciembre de 1978.
- ❖ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- ❖ Ley 5/2014, de 4 de abril, de Seguridad Privada.
- ❖ 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.
- ❖ Agencia Española de Protección de datos. (2025). *Guía sobre el uso de videocámaras para seguridad y otras finalidades*.
- ❖ Gobierno de España. (2021). *Carta de Derechos Digitales*.
- ❖ Comité Europeo de Protección de Datos. (2020). *Guidelines 3/2019 on processing of personal data through video devices*.

Jurisprudencia

Tribunal Constitucional de España

- ❖ Sentencia del Tribunal Constitucional 231/1988, de 2 de diciembre.
<https://www.boe.es/buscar/doc.php?id=BOE-T-1988-29203>
- ❖ Sentencia del Tribunal Constitucional 341/1993, de 18 de noviembre.
<https://www.boe.es/buscar/doc.php?id=BOE-T-1993-29248>
- ❖ Sentencia del Tribunal Constitucional 98/2000, de 10 de abril.
https://www.boe.es/diario_boe/txt.php?id=BOE-T-2000-9223
- ❖ Sentencia del Tribunal Constitucional 186/2000, de 10 de julio.
https://www.boe.es/diario_boe/txt.php?id=BOE-T-2000-15253
- ❖ Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.
<https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332>
- ❖ Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2013-2712
- ❖ Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2016-3405
- ❖ Sentencia del Tribunal Constitucional 119/2022, de 29 de septiembre.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-17975

Tribunal Supremo

- ❖ Sentencia del Tribunal Supremo de 26 de septiembre de 2007. <https://vlex.es/vid/on-i-re-31962968>
- ❖ Sentencia del Tribunal Supremo 77/2017, de 31 de enero.
<https://vlex.es/vid/670490065>
- ❖ Sentencia del Tribunal Supremo 398/2024. <https://vlex.es/vid/1028504074>

Tribunal Europeo de Derechos Humanos

- ❖ Tribunal Europeo de Derechos Humanos, asunto *Köpke c. Alemania*, decisión de 5 de octubre de 2010. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-101536%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-101536%22]})
- ❖ Tribunal Europeo de Derechos Humanos, asunto *López Ribalda y otros c. España*, Gran Sala, de 17 de octubre de 2019. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-189675%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-189675%22]})

Tribunal de Justicia de Unión Europea

- ❖ Sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-212/13, *Ryneš*, de 11 de diciembre de 2014. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62013CJ0212>

B) REFERENCIAS BIBLIOGRÁFICAS

- AEPD. (2025). *Guía sobre el uso de videocámaras para seguridad y otras finalidades*. Agencia Española de Protección de Datos.
- Álvarez de la Rosa, J.M., y Palomeque López, M.C. (2022). *Derecho del trabajo*. Editorial Universitaria Ramón Areces.
- Aragón Reyes, M. (2011). *Derechos fundamentales y su protección*. Madrid: Civitas.
- Ball, K. (2010). *Workplace surveillance: An overview*. Labor History, 51(1), 87-106.
- Baylos Grau, A. (2019). *Los derechos digitales y la negociación colectiva*. Diario La Ley, nº 9331.
- Baylos Grau, A. (2024). *Desequilibrio de poder en la empresa y entorno digital: la importancia de los derechos colectivos*.
- Brown, A. J. L., & O'Donnell, E. E. S. (2024). Big brother: The effects of surveillance on fundamental aspects of social vision. Scientific Reports, 14, 27508. <https://doi.org/10.1038/s41598-024-27508-0>
- Bygrave, A. L. (2014). *Data Privacy Law: An International Perspective*. Oxford, UK: Oxford University Press.

- Carazo Liébana, M. (2023). *El derecho fundamental a la protección de datos personales y la responsabilidad proactiva*. Aranzadi La Ley.
- De Hert, P., y Papakonstantinou, V. (2016). The new general data protection regulation: Still a sound system for the protection of individuals. *Computer Law and Security Review*, 32, 179–194.
- Ferrajoli, L. (2011). Constitucionalismo principialista y constitucionalismo garantista. *DOXA. Cuadernos de Filosofía del Derecho*(34), 15-53.
- Garriga Domínguez, A. (2009). *Tratamiento de datos personales y derechos fundamentales*. Dykinson.
- Gil Membrado, C. (2019). *Videovigilancia y protección de datos. Especial referencia a la grabación de la vía pública desde el espacio privado*. Wolters Kluwer España.
- Glavin, P., Bierman, A., & Schieman, S. (2024). Private eyes, they see your every move: Workplace surveillance and worker well-being. *Social Currents*, 11(4), 327–345.
<https://doi.org/10.1177/23294965241228874>
- Gobierno de España. (2021). *Carta de Derechos Digitales*.
<https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-carta-derechos-digitales.pdf>
- Martínez de Pisón, J. (2016). El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional. *Revista anuario de Filosofía del Derecho* (33).
- Molina Navarrete, C. (2019). La “gran transformación” digital y bienestar en el trabajo: Riesgos emergentes, nuevos principios de acción y nuevas medidas preventivas. *Revista de Trabajo y Seguridad Social. CEF*, (438), 5-44.
- Pandey, S. K., & Pravesh, R. (2025). Workplace surveillance and its psychological impacts of on employee: A review. *OPUS*, 16(1), 18–35.
- Pérez de los Cobos Orihuel, F. (2018). *El derecho al respeto de la vida privada: los retos digitales*. Consejo de Europa.
- Pérez Luño, A. (1999). *Derechos Humanos, Estado de Derecho y Constitución*. Editorial Tecnos.

- Polo Roca, A. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político*, 1(108), 165-194. <https://doi.org/https://doi.org/10.5944/rdp.108.2020.27998>
- Velásquez Espinoza, G. E., y Román Armijos, R.A. (2024). Análisis constitucional sobre la vulneración al derecho a la intimidad por el monitoreo de cámaras en lugares públicos y privados. *Ltam: revista latinoamericana de Ciencias Sociales y Humanidades*, 5(3).
- Volosevici, D., & Iacobescu, G. D. (2025). Surveillance as a socio-technical system: Behavioral impacts and self-regulation in monitored environments. *Systems*, 13, 614. <https://doi.org/10.3390/systems13090614>
- Zuboff, S. (2019). *La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder*. Paidós.

Declaración sobre el uso de herramientas de Inteligencia Artificial

Para la realización del presente Trabajo Fin de Grado se ha utilizado la herramienta de inteligencia artificial ChatGPT (OpenAI) como apoyo complementario en tareas de mejora de redacción, organización de contenidos, aclaración de conceptos jurídicos y orientación en la localización y estructuración de información doctrinal y jurisprudencial.

No obstante, el contenido final del trabajo ha sido revisado, contrastado y desarrollado bajo criterio propio del autor, quien asume plenamente la responsabilidad sobre su contenido y conclusiones.

Del mismo modo, durante el uso de dichas herramientas no se han introducido datos personales ni información sensible, siguiendo las directrices establecidas por la Universidad Miguel Hernández de Elche sobre el uso de inteligencia artificial generativa.