Universidad de Valladolid

Facultad de **Derecho**

Máster en Abogacía y Procura

icava
Ilustre Colegio de Abogados de Valladolid

Investigación interna en las personas jurídicas: videovigilancia y control de las comunicaciones.

Presentado por:

Luis Obispo Arranz

Tutelado por:

Oliver Pascual Suaña

Valladolid, 21 de febrero de 2025

ÍNDICE

Resumen:

Las medidas de vigilancia y control en el ámbito laboral son herramientas imprescindibles para garantizar la seguridad y el correcto desarrollo de la actividad empresarial. No obstante, su implantación puede plantear conflictos laborales. Para una correcta adopción, se requiere garantizar el equilibrio entre el ejercicio de esta prerrogativa por parte del empresario y los propios derechos de los trabajadores.

Dada la naturaleza interpersonal de la relación laboral, cuando de la adopción de estas medidas se infiere un desequilibrio de posiciones, puede producirse la vulneración de derechos de los trabajadores y, consecuentemente, provocar conflictos, tanto en el entorno laboral como en sede judicial.

Es por ello que este trabajo buscará determinar hasta dónde puede llegar el empresario en su facultad de supervisión, qué garantías deben respetarse para evitar la vulneración de derechos fundamentales, así como estudiar las consecuencias de utilizar, en el régimen sancionador o en ámbito judicial, pruebas obtenidas con la inobservancia de estas garantías.

Palabras clave:

Poder de dirección y control, empresa, empresario, trabajador, vigilancia, videovigilancia, proporcionalidad, derechos de los trabajadores, vulneración.

Abstract:

Surveillance and control measures in the workplace are essential tools adopted by the employer to guarantee safety and the correct development of his activity. However, their implementation may give rise to labour conflicts. For their effective adoption, proper advice is required to ensure a balance between the exercise of this right by the employer and the workers' own rights.

Given the interpersonal nature of the employment relationship, when the adoption of these measures leads to an imbalance of rights, this can lead to infringements of workers' rights and, consequently, to conflicts, both in the workplace and in the courts.

It is therefore essential to determine how far the employer can go in his supervisory powers and what guarantees must be respected in order to avoid the infringement of fundamental rights, as well as to study the consequences of using evidence obtained in breach of these guarantees in the sanctioning system or in the judicial sphere.

Key Words:

Power of direction and control, company, businessman, worker, surveillance, video surveillance, proportionality, workers' rights, violation

ABREVIATURAS

CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
ET	Estatuto de los Trabajadores
FD	Fundamentos de derecho
LECrim	Ley de Enjuiciamiento Criminal
LOPD	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales
LOPJ	Ley Orgánica del Poder Judicial
LRJS	Ley Reguladora de la Jurisdicción Social
OIT	Organización Internacional del Trabajo
RLT	Representante legal de los trabajadores
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
STSJ	Sentencia del Tribunal Superior de Justicia
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TS	Tribunal Supremo

1. INTRODUCCIÓN

Se presenta un supuesto donde un trabajador es sorprendido por las cámaras de videovigilancia de la entidad en la que presta servicios, sustrayendo un artículo personal de la mochila de un compañero. Este hecho activa una investigación empresarial interna, gracias a la cual, se descubre un ilícito que lleva cometiéndose de forma continuada durante los últimos meses.

Para un examen completo es necesario desarrollar el marco normativo que regula estas medidas de dirección y control en el contexto laboral – siendo la videovigilancia elemento nuclear del supuesto –; prestar atención a la legislación vigente en materia laboral, como es el E.T. y la LOPD; a las previsiones constitucionales; así como a la doctrina jurisprudencial sentada, principalmente por el TS y el TEDH, que, dada la naturaleza cambiante del derecho laboral, fija constantemente precedentes para la resolución de los conflictos entre ambas partes.

En el trabajo se profundizará en sentencias relevantes que han supuesto un verdadero punto de inflexión en la materia, con especial interés en las dictadas por los órganos nacionales en relación con los "casos Bershka" y "Falciani", y a las del TEDH en los asuntos "López Ribalda" y "Barbulescu".

En este sentido, el análisis aborda los límites y condiciones que la legislación impone a los empresarios en la adopción de medidas de vigilancia, ponderando su necesidad, proporcionalidad y respeto a los derechos de los trabajadores: sobresalen al respecto el derecho a la intimidad y el secreto de las comunicaciones.

2. ANTECEDENTES DE HECHO

RECAUCHUTADOS MIGUEL ÁNGEL, S.L. ("RECAUCHUTADOS"), es una sociedad limitada cuya actividad principal es la fabricación de neumáticos, cámaras de caucho y todo lo relacionado con la reconstrucción y recauchutado de los mismos.

La mercantil, con centro de trabajo en Valladolid, cuenta con una plantilla conformada por sesenta y siete trabajadores, cincuenta y cuatro de los cuales desempeñan su actividad con un ritmo productivo ininterrumpido distribuido en tres turnos rotativos con los siguientes horarios:

- 7:00h a 15:00h
- 15:00h a 23:00h
- 23:00h a 7:00h

Para contextualizar con exactitud los acontecimientos que motivan el desarrollo de este trabajo, es preciso describir, además de los concretos comportamientos que justifican la investigación empresarial, el lugar y las circunstancias temporales de los hechos objeto de análisis.

RECAUCHUTADOS cuenta con una amplia infraestructura que le permite mantener una producción muy elevada, siendo una de las empresas nacionales con más competitividad y volumen de trabajo.

Sus instalaciones están organizadas por diferentes áreas. Una "zona principal" de trabajo, dividida a su vez por cinco espacios o "subáreas". Para acceder a la zona principal, y a las subáreas, los trabajadores tienen que pasar por unas puertas de seguridad.

Tanto en la entrada de la zona principal como en la de cada una de las subáreas, constan instaladas cámaras de videovigilancia. En los contratos individuales de cada trabajador se incluyen una cláusulas especificas que establecen la advertencia de la captación de imágenes en el ámbito laboral, y su destino para el control del correcto desarrollo de la actividad de la empresa; informándose a los empleados que estas videocámaras actúan como una herramienta de control de la actividad, de manera que, si se constata la existencia de

incumplimientos laborales, se podrán comprobar por medio del visionado de las grabaciones.

Además de las zonas de trabajo descritas, las instalaciones de la entidad cuentan con otros espacios necesarios para el desarrollo diario de la actividad como son: las conocidas "salas de descanso", los vestuarios, aseos, comedores, despachos del personal administrativo y, por lo que aquí nos ocupa, diferentes zonas de almacenaje.

Las zonas de almacenaje se localizan cerca de la entrada a la zona principal de trabajo y, por tanto, en la parte *inicial* de la actividad productiva de la entidad. Estas zonas permiten el depósito de utensilios de oficina, pequeñas herramientas de trabajo y material plástico propio para el tratamiento del neumático, facilitando su reposición continua y rápida en las zonas de trabajo habilitadas para su manipulación.

En atención a la ubicación de estas zonas de almacenaje y su conexión directa con las zonas de trabajo efectivo, es habitual que los trabajadores, pese a no ser su destino inicial, las aprovechen para depositar pequeñas mochilas con alimentos y enseres personales, facilitando su recogida a la hora de acudir a las salas de descanso y maximizando así su tiempo de asueto.

Esta práctica es conocida por la empresa, por ello, se ha insistido reiteradamente desde la dirección que se trata de una zona de almacenaje productivo y, en consecuencia, de uso únicamente laboral, por lo que no está permitido, en ningún caso, la estancia en esa ubicación para descansar, conversar o ingerir los alimentos allí depositados, es decir, utilidades distintas a la finalidad de la misma, almacenaje y reposición del material. Esta advertencia viene reflejada en el régimen interno legalmente elaborado por la empresa, pues en alguna ocasión, se han producido distorsiones en la actividad diaria de la misma como resultado de las molestias generadas por trabajadores que las empleaban para descansar, viéndose obligada la empresa a realizar las consecuentes amonestaciones.

Efectuado este análisis de la mercantil, sus instalaciones y desarrollo productivo, hay que centrarse en los hechos que han motivado la consulta de la sociedad RECAUCHUTADOS a nuestro departamento jurídico.

En los últimos meses se vienen repitiendo desfases en el registro de entrada y salida del material plástico apilado en estas zonas de almacenaje, sospechando que, detrás de esta problemática, no hay un error logístico sino la concurrencia de una serie de actos ilícitos.

Sin embargo, dado que la cantidad de material sustraído no es relevante en comparación con el volumen de uso mensual, la sociedad optó por una posición pasiva, no incoando, inicialmente, investigaciones al respecto.

No obstante, el hecho detonante que puso en alerta a la dirección de la empresa fue la denuncia de uno de los trabajadores del turno de noche, en la que se manifestaba la desaparición de un utensilio personal depositado en la zona de almacenaje.

Este hecho ocurrió el día 17 de diciembre de 2024 a las 4:00h.

En esta fecha, una vez concluida la jornada laboral del trabajador D. Iván Cantalejo, al recoger sus pertenencias depositadas en la zona de almacenaje se percató que, entre las mismas, no se encontraba una pequeña navaja que siempre lleva consigo por su utilidad para la pausa del bocadillo, y su valor personal. El trabajador preguntó al resto de compañeros de turno, que niegan conocer su paradero, y al no localizar la navaja, decidió poner esta circunstancia en conocimiento de la dirección de la empresa por medio del sistema interno de información ("canal de denuncias") implantado en esta.

Una vez tiene conocimiento de este suceso, la entidad decide visualizar las cámaras de seguridad de la zona concreta, en la fecha indicada, percatándose de que son tres los trabajadores que, aprovechando el cambio de turno, se acercan a la estantería donde, efectivamente, se encontraba la mochila de D. Iván. Uno de ellos, D. Daniel Becerro[1], perfectamente identificable mediante las imágenes captadas por las cámaras, introdujo la mano en uno de los bolsillos laterales de la mochila propiedad de D. Iván, extrayendo el artículo de la misma, e introduciéndolo en el bolsillo derecho de su pantalón mientras alardea ante sus dos compañeros de la "hazaña" consumada.

[1] Este trabajador cuenta con una larga trayectoria en la empresa, y compagina sus funciones de operario con las de jefe de turno. Por este motivo, cuenta con un ordenador portátil facilitado por la empresa, y correo electrónico corporativo, destinados a la gestión de los turnos propios y de sus subordinados, a la comunicación y coordinación con el equipo de dirección y de cualquier otra gestión relativa a sus funciones.

Este hecho y la consecuente denuncia del Sr. Cantalejo formulada al día siguiente de los hechos (18 de diciembre de 2024), supuso el inicio de una investigación interna, en el seno de la cual se produjo el visionado de los videos captados por las cámaras de seguridad con el convencimiento de que ese desfase en el material plástico se debía a pequeños y sucesivos hurtos realizados por trabajadores.

Tras una visualización exhaustiva, la entidad descubre que este desfase se debe a numerosas sustracciones realizadas por el mismo trabajador responsable de la desaparición de la navaja, el Sr. Becerro, que aprovechaba los momentos en los que salía de las instalaciones a fumar (está prohibido fumar en las instalaciones por el riesgo de incendio asociado al tratamiento del caucho) o a "tirar" la basura, para ocultarla junto a la mercancía sustraída y depositarla en su vehículo aparcado en las inmediaciones de las instalaciones.

Una vez la empresa es conocedora de los hechos reales, considera que se debe despedir al Sr. Becerro, si bien, se plantean la necesidad de continuar con la investigación interna y acceder a su correo electrónico corporativo con la finalidad de buscar información relevante sobre los ilícitos; y justificar, más si cabe, la extinción de la relación laboral y las consecuentes responsabilidades que sus actos pudieran estar generando. Se sospecha que el denunciado se aprovecha de su condición de jefe de turno, y el consecuente acceso al sistema informático de la empresa, para emplear el email corporativo y facilitar la transmisión a terceros del material sustraído.

Ante esta disyuntiva la empresa decide ser cauta y, antes de proceder al despido del trabajador, acude a nuestro servicio jurídico solicitando asesoramiento en tal sentido, al objeto de conocer:

(i) si existe la opción de acceder al correo corporativo del trabajador para intentar conseguir más indicios que acrediten la comisión de los ilícitos objeto de investigación;

(ii) la posibilidad de sustentar el despido en las imágenes obtenidas con las cámaras instaladas en las instalaciones;

(iii) si en consecuencia puede ser efectivamente despedido por la sustracción de la navaja y del material plástico, tal y como captaron las imágenes y;

(iv) la necesidad, o no, de dar audiencia previa al trabajador o de llevar a cabo una consulta con el comité de empresa – expediente contradictorio –;

3. FUNDAMENTOS DE DERECHO

3.1. PODER DE DIRECCIÓN Y CONTROL EMPRESARIAL SOBRE LOS TRABAJADORES EN EL ENTORNO LABORAL.

La relación entre empresario y trabajador se caracteriza por su asimetría jurídica. El empleado presta sus servicios en una posición de subordinación, mientras que el empresario ostenta un poder de dirección que le permite organizar y controlar la actividad laboral. Este poder fundamentado en la libertad de empresa – *ex.* art. 38 C.E. – es esencial para asegurar el funcionamiento de la entidad y la consecución de sus objetivos económicos. El poder de dirección [2] surge del contrato laboral, y se traduce en la facultad del empresario de determinar cómo se realiza la prestación del trabajo, los medios a emplear, los resultados esperados, y las medidas de control[3] efectivo sobre la actividad de los trabajadores, limitando así la autonomía de estos.

En estos términos, el artículo 20.3 E.T. le otorga al empresario la potestad de *"adoptar las medidas que considere más oportunas de vigilancia y control a efectos de verificar que los trabajadores cumplen con sus obligaciones y deberes laborales, siempre guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad"*. Un ejemplo de medida de vigilancia y control relativa a la potestad fiscalizadora se manifiesta en la posibilidad de registrar las

[2] El artículo 5.c E.T. establece que para que el ejercicio del poder de dirección sea susceptible de generar un deber de obediencia en el trabajador es necesario que este sea regular.

[3] En el supuesto de hecho, las medidas de vigilancia y control que adopta la entidad se limitan a la instalación de cámaras de videovigilancia con la información previa y necesaria a los trabajadores para cumplir con toda la normativa vigente.

taquillas y efectos particulares "*cuando sea necesario para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa"*.[4]

El resultado de estas medidas fiscalizadoras es el poder disciplinario del propio empresario y, en su caso, la facultad de sancionar a los trabajadores por los incumplimientos laborales, de acuerdo con la graduación de faltas y sanciones que se establezcan en las disposiciones legales o en el convenio colectivo de aplicación.[5]

Un aspecto importante dentro de este poder empresarial es lo que se conoce como «*ius variandi*» del empresario, esto es, la facultad de modificar unilateralmente ciertas condiciones laborales, funcionales o geográficas dentro de los límites legales establecidos. Sin embargo, el ejercicio de este poder no es ilimitado y debe respetar los derechos fundamentales del trabajador, su dignidad, intimidad y libertad ideológica, así como los derechos laborales pactados. Las normas sobre jornada de trabajo, descansos, seguridad e integridad física también actúan como límites a este poder. En caso de órdenes abusivas o ilegales, la jurisprudencia ha reconocido que el trabajador puede desobedecerlas si existe un abuso de derecho por parte del empresario.

Asimismo, en la actualidad, esta limitación al poder de control está reforzada en los supuestos – como el caso que se trata – de uso de dispositivos de videovigilancia que puedan afectar al derecho a la intimidad de los trabajadores. Resultan aquí de aplicación los preceptos establecidos, principalmente, en la LOPD, que especifica en sus arts. 87 a 91 el alcance de esa protección en materia laboral [6].

En definitiva, el empresario ejerce un poder de dirección reglado, amplio en su alcance, pero sujeto a los límites impuestos por los derechos del trabajador, la legislación laboral y los acuerdos colectivos.[7]

---

[4] Esta previsión se recoge en el artículo 18 E.T., y debe realizarse cumpliendo unas garantías: ha de llevarse a cabo dentro del centro de trabajo, en horas de trabajo, y en presencia de un representante legal de los trabajadores, o en su ausencia, de otro trabajador de la empresa siempre que ello fuera posible; asimismo, este precepto, como el artículo 20.3 E.T., impone que la intromisión debe respetar la dignidad e intimidad del trabajador.

[5] Art. 58.1 E.T.

[6] Art. 20 bis E.T.

[7] MARTÍN VALVERDE, A., RODRÍGUEZ-SAÑUDO GUTIÉRREZ, F., GARCÍA MURCIA, J. "Posición jurídica del empresario en el ordenamiento laboral", *Derecho del Trabajo,* 29º edición, Tecnos, Madrid, 2020, pp. 264-269.

3.2. INVESTIGACIONES INTERNAS EN EL ÁMBITO EMPRESARIAL. COMPLIANCE *AD INTRA*.

Cuando las medidas preventivas de control empresarial no son efectivas y existen indicios de la comisión de ilícitos en el seno de la entidad, se deben llevar a cabo las denominadas investigaciones internas. Estas indagaciones, insertas *de facto* en el poder de dirección y control empresarial, juegan un papel esencial en el cumplimiento normativo y la protección de las empresas frente a conductas irregulares de sus subordinados y terceros relacionados.

Las investigaciones internas se pueden calificar como las "*actividades de obtención y aportación de información, indicios y pruebas, llevadas a cabo de forma privada (por su propia iniciativa), orientadas a la averiguación y esclarecimiento de unos determinados hechos acaecidos en el seno de la empresa, que pudieran suponer actos delictivos, irregularidades, contravenir el código ético de la compañía o representar un riesgo para su normal funcionamiento*". [8]

Para el inicio de una investigación de este tipo, no es imprescindible contar con un protocolo previamente establecido, pero sí resulta recomendable que las entidades dispongan de políticas internas que detallen los procedimientos de actuación. Políticas que deben incluir los derechos laborales y fundamentales de los empleados, prestando especial atención al respeto por la intimidad y al secreto de las comunicaciones – como se expondrá en epígrafes correspondientes – por ser derechos susceptibles de vulneración en estos procedimientos.

Un papel fundamental dentro las investigaciones lo ostentan los propios trabajadores de las entidades. Diversos estudios estadísticos[9] establecen que alrededor del 40% de los delitos de fraude cometidos en empresas se detectan gracias a las denuncias realizadas a través de canales internos, lo que subraya la eficacia de estas herramientas.

---

[8] MARTÍN POLVORINOS, C. *"Las investigaciones internas corporativas desde la perspectiva de la investigación privada"*. World Compliance Association, 2021 [En línea] https://bibliotecacompliance.com/wp-content/uploads/2021/02/FASC-2_INVESTIGACIONES-INTERNASpdf.pdf [consulta: 18 nov. 2024]

[9] Association of Certified Fraud Examiners *Occupational Fraud 2024: A report to the nations.* [En línea]. https://legacy.acfe.com/report-to-the-nations/2024/ [consulta: 18 nov. 2024]

Muestra de esta relevancia es la Directiva Europea 1937/2019, para la protección de las personas que informen sobre infracciones del Derecho de la Unión, denominada «Directiva *Whistleblower»*. Esta norma europea, traspuesta en España mediante la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, ha consolidado un marco normativo para la protección de los denunciantes y la gestión de investigaciones internas. Su objetivo principal es asegurar que cualquier trabajador[10] disponga de un instrumento que le permita revelar acciones u omisiones que puedan ser constitutivas de infracciones graves o muy graves, o vulneraciones – de cualquier ordenamiento jurídico – que ocurran en su empresa, garantizando, entre otros aspectos, su anonimato o confidencialidad, puesto que la protección del denunciante es el principio fundamental. Este instrumento alude a los referidos sistemas internos de información para poner en conocimiento de la organización aquellas infracciones detectadas, aplicando ciertas garantías al denunciante.[11]

Las investigaciones internas[12] permiten a las entidades recopilar información crucial sobre los hechos ocurridos en su seno, fortaleciendo su derecho de defensa, y demostrando la eficacia de los sistemas de cumplimiento. Para maximizar su efectividad en los supuestos iniciados a instancia de un trabajador denunciante, estas deben seguir procedimientos[13] rigurosos desde la recepción de la denuncia hasta la conclusión de la investigación.

---

[10] El ámbito de aplicación de la Ley 2/2023, de 20 de febrero, se regula en su artículo 3, cuyo apartado primero establece que, de forma general, será de aplicación a los informantes que trabajen en el sector privado y hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso a los trabajadores por cuenta ajena.

[11] PASCUAL SUAÑA, O. *Defensa de las personas jurídicas en el proceso penal español. Especial referencia a los informes periciales de compliance.* Tirant lo Blanch, Valencia, 2024.

[12] El artículo 8.5 de la Directiva *Whistleblower*, que reconoce la obligación de establecimiento de canales de denuncia interna, admite la posibilidad de que la gestión del sistema de denuncias se delegue en asesores externos, proporcionando esta alternativa mayor imparcialidad y protección en el resultado de las indagaciones.

[13] El inicio del proceso se produce con la recepción de una denuncia a través de la vía establecida a tal efecto. Si la denuncia se admite a trámite, se abrirá un expediente y comenzará la investigación de acuerdo al protocolo establecido por la empresa (recopilación de pruebas, análisis de información, entrevista con denunciante, testigos, etc). En caso de ser necesario, se resolverá el expediente con las medidas disciplinarias a aplicar y la comunicación con las autoridades correspondientes. La elaboración del informe final es el paso culminante del proceso, donde se recogen los hallazgos, las conclusiones y las recomendaciones para prevenir futuros incumplimientos. La obligatoriedad de mantener un registro detallado de las denuncias y su gestión es otro elemento clave para demostrar la eficacia del sistema de cumplimiento de la organización, de acuerdo con el artículo 24 LOPD. Es imprescindible que las personas encargadas de estas tareas posean formación

En conclusión, las investigaciones internas son una herramienta indispensable para las empresas en la detección y prevención de conductas irregulares (*ad intra*[14] *y ad extra),* así como para la protección de los derechos de todas las partes involucradas. La adecuada gestión de estas investigaciones fortalece la cultura corporativa, mejora la transparencia, y minimiza los riesgos legales, evitando la responsabilidad de la empresa ante vulneraciones normativas y su posible responsabilidad penal en determinados delitos.[15]

3.3. DERECHOS AFECTADOS POR LAS INVESTIGACIONES INTERNAS.

3.3.1. Punto de partida.

Como se ha referido con anterioridad, el empresario, en el ejercicio del poder de dirección, está facultado para adoptar medidas de control destinadas a verificar el correcto desarrollo de la actividad laboral de los trabajadores. Decisiones como la instalación de sistemas de videovigilancia, la geolocalización, el monitoreo de equipos informáticos, los correos electrónicos y la navegación en internet, son instrumentos que van a proporcionar un análisis detallado del rendimiento laboral de los trabajadores. Esto incluye parámetros como la cantidad y calidad de las tareas ejecutadas; el tiempo empleado; las interrupciones y su frecuencia; los patrones conductuales e, incluso, rasgos personales de los empleados como sus preferencias, ideología, estilo de vida o predisposición a enfermedades. En esencia, estas tecnologías permiten una trazabilidad exhaustiva de las conductas actuales y futuras de los trabajadores.

De este modo, los controles empresariales son susceptibles de revelar incumplimientos laborales, por lo que, ante la sospecha de su concurrencia, es común que los empresarios inicien investigaciones internas para esclarecer los hechos y aplicar, si procede, las sanciones oportunas.

---

especializada y actúen con imparcialidad. GRUPO ÁTICO 34 *Procedimiento del Canal de Denuncias*. 2024 [En línea] https://protecciondatos-lopd.com/empresas/compliance/canal-denuncias/procedimiento/#Como_debe_ser_el_procedimiento_del_canal_de_denuncias_de_una_empresa [consulta: 18 enero 2025]

[14] STS núm. 338/2019, de 3 de julio.

[15] PASCUAL SUAÑA, O., "Mejores prácticas en los canales de denuncias", *Revista Brasileira de Direito Processual Penal,* Vol. 9, Nº. 2, 2023, pp. 575-607 (Vista do Mejores prácticas en los canales de denuncias)

Este fenómeno plantea un punto crítico en la gestión automatizada de datos de los empleados, puesto que, a pesar de que las vigilancias mencionadas resulten altamente beneficiosas para la toma de decisiones estratégicas, su propia aplicación y las consecuentes investigaciones y sanciones implican riesgos significativos para con los trabajadores, pudiendo lesionar diferentes derechos fundamentales.[16]

Al respecto, resulta indiscutido que el trabajador por cuenta ajena es titular de un haz de derechos fundamentales reconocidos en la C.E. y en otros instrumentos supranacionales[17], siendo este aspecto relevante puesto que cualquier vulneración grave de estos podría invalidar los resultados obtenidos.

En referencia a las medidas adoptadas y a la investigación ejecutada en el supuesto concreto – visualización y uso de imágenes captadas por cámaras de videovigilancia y el acceso al correo corporativo –, según el criterio de LASCURAÍN SÁNCHEZ[18] y PASCUAL SUAÑA[19] entre otros (que aquí se comparte), debe aplicarse a las investigaciones en entornos empresariales la doctrina de la *prueba prohibida* [20], equiparándolas al proceso penal y excluyendo las pruebas obtenidas con vulneración de derechos fundamentales.

En definitiva, la captación de imágenes por cámaras de videovigilancia (y su utilización para justificar una sanción) o el posible acceso a los correos electrónicos corporativos, va a

---

[16] RODRÍGUEZ ESCANCIANO, S. *"*Videovigilancia de seguridad como prueba de ilícitos laborales ante sospecha de comportamiento irregular*", Revista de Jurisprudencia Laboral.* Número 10/2022. pp.1-2.

[17] Fundamentalmente los previstos en la Carta de Derechos Fundamentales de la Unión Europea y en el Convenio Europeo de Derechos Humanos.

[18] LASCURAÍN SÁNCHEZ, J.A. "La responsabilidad penal individual por los delitos de empresa" en NIETO MARTÍN, A (Dir), LASCURAÍN SÁNCHEZ, J.A., BLANCO CORDERO, I., PÉREZ FERNÁNDEZ, P., GARCÍA MORENO, B (Coords). *Manual de cumplimiento penal en la empresa.* Tirant lo Blanch, Valencia, 2015. p. 270.

[19] PASCUAL SUAÑA, O. Defensa de las personas jurídicas... ob. cit. p.136.

[20] COLMENERO GUERRA, J.A. "La prueba ilícita". Tomo IV. *La prueba en el proceso laboral*. Tirant lo Blanch, Valencia, 2017, p.107. Obra donde el citado autor hace referencia a este concepto. Por prueba prohibida habrá que entender las infracciones de derechos relevantes, fundamentales o no, producidas en la obtención de la fuente de prueba. Es decir, en la obtención de la prueba pueden vulnerarse derechos y libertades fundamentales, y otros que no poseen dicho rango, pero la vulneración de estos últimos no supone que la prueba sea necesariamente ilícita. Ahora bien, las vulneraciones producidas en la obtención de las fuentes de prueba, que afecten a derechos y libertades fundamentales, son una actividad prohibida por la ley – art 283.3 LEC y art. 90.2 LRJS – y va a verse afectado el concreto medio de prueba en que se ha producido la vulneración y los que traen causa de este.

afectar a los siguientes derechos[21], siempre y cuando no se realice cumpliendo todas las garantías exigidas y analizadas en epígrafes posteriores:

3.3.2 El secreto de las comunicaciones.

La evolución de las comunicaciones tecnológicas con el empleo de correos electrónicos, mensajes de texto, mensajería instantánea – *WhatsApp* principalmente – como medio habitual de interacción, hace que la forma de intercambiar información sea muy variada; diversidad, por supuesto, presente en todos los ámbitos de la actividad laboral.

En la misma medida que el empleo de estos medios facilita la comunicación entre los propios trabajadores, aporta al empresario una fuente de información en la búsqueda de incumplimientos laborales.

Ahora bien, las comunicaciones que se realizan a través de estas vías, con una serie de condicionantes a tener en cuenta, están protegidas por el secreto de las comunicaciones – *ex.* art. 18.3 C.E. – siendo clave en la contextualización de esta prerrogativa constitucional la STC núm. 70/2002, de 3 de abril.

En este asunto, el TC define el secreto de las comunicaciones como *"una plasmación singular de la dignidad de la persona y el libre desarrollo de la personalidad que son fundamento del orden político y la paz social (artículo 10.1 CE), por lo que la comunicación es a efectos constitucionales el proceso de transmisión de expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos".* Igualmente, hace una referencia al concepto de comunicación, y es que, dada la referida evolución tecnológica, es imperativo

[21] CHARRUTTI GARCÉN, M.L., "Límites jurídicos al poder de dirección del empleador en el uso de nuevas tecnologías digitales de la información y la comunicación. Un estudio desde los derechos fundamentales del trabajador" en LÓPEZ AHUMADA (Dir), JIMENEZ MARTÍNEZ, M.V., ROLDÁN MARTINEZ (Coords), *La garantía de los derechos digitales en el ámbito laboral: políticas empresariales, ejercicio de derechos y límites al poder de control del trabajo,* Aranzadi, Navarra, 2023. pp. 154-157. Destaca este autor que, ante el uso de las nuevas tecnologías en el ámbito laboral, surge el interrogante de saber cuáles son los derechos que pueden verse afectados, entendiendo además del secreto de las comunicaciones y la intimidad, el derecho a la protección de datos – art. 18.4 C.E. – y el derecho al respeto de la vida privada y familiar (art. 8 CEDH).

adaptar este concepto de comunicación y su objeto de protección como derecho fundamental para que esa protección se extienda a los nuevos ámbitos.[22]

De este modo, el secreto abarca cualquier forma de transmisión de información, extendiéndose a los nuevos medios digitales, y protegiendo, tanto el contenido como la identidad de los comunicantes[23].

La jurisprudencia – por todas, STC núm. 98/2000, de 10 de abril – establece que cualquier restricción al secreto de las comunicaciones debe cumplir con el criterio de proporcionalidad, teniendo cabida si no existen alternativas menos invasivas.[24]

En relación con la cuestión planteada por RECAUCHUTADOS sobre la posibilidad de acceder al correo corporativo del trabajador investigado, con carácter general, la captación de correos o mensajes no leídos sin autorización judicial vulnera el derecho referido y por ende, la prueba obtenida será considerada prohibida – *ex.* art. 11.1 LOPJ[25] –. Ello sin perjuicio de las opciones a las que se hará referencia para romper la denominada expectativa de privacidad y poder acceder a los emails, cumpliendo ciertas garantías, sin infringir derecho alguno.[26]

3.3.3. Derecho a la intimidad.

El derecho a la intimidad es un derecho fundamental reconocido en el artículo 18.1 C.E. y en el artículo 8 CEDH. Protege aspectos propios de la esfera física y fisiológica de las personas, de su esfera psicológica e intelectual, familiar, y otras facetas de las propias relaciones personales, abarcando toda la vida privada de aquellas. Al respecto, el TEDH adopta una interpretación amplia del concepto de vida privada[27], estableciendo que el término "vida privada" posee un contenido extenso y no susceptible de una definición exhaustiva. Destaca que la protección ofrecida por el artículo 8 del CEDH alcanza más allá

[22] F.D. 3º y 9º.
[23] STC núm. 114/1984, de 29 de noviembre.
[24] Cuestión sobre la que se profundiza en el epígrafe 3.6, correspondiente al "acceso al correo corporativo del investigado".
[25] Este precepto establece las consecuencias de una prueba denominada prohibida, y es que *"no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales"*.
[26] PASCUAL SUAÑA, O. Defensa de las personas jurídicas …ob cit. pp.137-139.
[27] Tras el fallo de la Gran Sala de 5 de septiembre de 2017 en el caso Barbulescu c.Rumanía.

del círculo íntimo de la persona, extendiéndose también al entorno laboral[28], como asimismo establece el E.T. en su artículo 4.2.e)[29].

En relación con este derecho debe resaltarse la STC núm. 77/2009, de 23 de marzo, y la STS (Sala 4º) núm. 966/2006, de 26 de septiembre [30].

De forma genérica, el TC manifiesta que este derecho *"confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido"* [31]. Esa prerrogativa se mantiene en el seno de la relación laboral, puesto que el trabajador no puede verse despojado del ejercicio y el respeto de este derecho fundamental, sin perjuicio de su posible modulación para equilibrar los intereses de los trabajadores y de los empresarios, *"en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva"* [32].

En determinadas circunstancias, este equilibrio se produce con las medidas de vigilancia y control[33] implantadas por el empresario, y con la efectiva realización de las investigaciones internas a las que nos hemos referido. Sin embargo, estas prácticas empresariales generan infinidad de controversias. Ante esta disyuntiva, el Alto Tribunal ha asentando la doctrina, señalada en el epígrafe anterior, sobre la *«expectativa razonable de intimidad»*, necesaria para el correcto desarrollo de aquellas, manifestando que *"lo que debe de hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios – con aplicación de prohibiciones absolutas o parciales – e informar a los trabajadores de que va a existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para*

---

[28] GALLARDO MOYA, R. "Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5 de septiembre de 2017 en el caso Barbulescu c. Rumania". *Revista de derecho social* 79 Bomarzo, Albacete, 2017, p.145. Noción compartida por la autora, quien refiere, en relación con el artículo 8 CEDH, que el derecho a la intimidad persiste en contextos públicos, y que debe incluirse en el ámbito laboral.

[29] "*En la relación de trabajo, los trabajadores tienen derecho al respeto de su intimidad"*.

[30] PASCUAL SUAÑA, O. Defensa de las personas jurídicas … ob cit. p.139.

[31] STC núm. 77/2009, de 23 de marzo, F.D.2º.

[32] STC núm. 151/2004, de 20 de septiembre, F.D.7.

[33] Art. 20.3 E.T.: *"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad"*.

garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, con la exclusión de determinadas conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado «una expectativa razonable de intimidad» [34].

Concretamente, además de por su relevancia y por la vinculación con el caso, hay que señalar que este derecho está estrechamente relacionado con la videovigilancia en el ámbito laboral regulado por el artículo 89.1 LOPD. Este precepto, complementado con la facultad que otorga el Estatuto para implementar medidas de control al respecto, regula el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos, habilitando el uso de cámaras a los empresarios siempre y cuando cumplan con la información previa, clara y concisa a los trabajadores o a sus representantes.

No obstante, a pesar de estas facultades para implementar control a través de cámaras de videovigilancia, existen límites inquebrantables. Por ejemplo, está prohibido instalar cámaras en zonas de descanso o esparcimiento, como vestuarios, aseos o comedores. Además, el uso de estos dispositivos debe regirse por los principios de proporcionalidad, necesidad e idoneidad.

Asimismo, suele ser suficiente para cumplir con la obligación de información, incluso sin una notificación específica para cada trabajador, la colocación de carteles visibles[35] en lugares estratégicos, fundamentalmente, en los casos donde se detecta la comisión flagrante de actos ilícitos, siempre que estos indiquen claramente la finalidad de la videovigilancia.

Estos términos vienen previstos en el artículo 89.1 LOPD, ya que su segundo párrafo hace alusión al cumplimiento de este deber de información con la mera existencia de los dispositivos a los que se refiere el artículo 22.4[36] del mismo texto legal para los casos de captación de delitos flagrantes.[37]

---

[34] STS núm. 966/2006, de 26 de septiembre de 2007. F.D. 4º.

[35] Deber de información que se entiende cumplido tras la STC núm. 39/2016, de 3 de marzo, conocida como "Caso Bershka", y que será objeto de análisis en epígrafes posteriores.

[36] Art. 22.4 LOPD: "*El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del*

En cuanto al consentimiento del trabajador, no parece necesario cuando el objetivo de la videovigilancia es la seguridad o el control laboral, ya que se presume implícito en la relación contractual. Sin embargo, el principio de proporcionalidad se convierte en la piedra de toque para determinar la legitimidad de las medidas empresariales, aunque su interpretación subjetiva puede dar lugar a discrepancias entre los órganos judiciales.[38]

Concluyendo, es fundamental cumplir con estos principios en las medidas de control, debiendo estar correctamente reflejados en los protocolos empresariales, pues, de lo contrario, las pruebas obtenidas por la aplicación de estos medios serán prohibidas y, consecuentemente nulas – *ex*. art. 11.1 LOPJ –.

3.3.4. Derecho al entorno digital y a la protección de datos.

Estrechamente relacionados con el derecho a la intimidad y susceptibles de ser fácilmente vulnerados en un supuestos como el de RECAUCHUTADOS, se encuentran: el derecho fundamental al entorno digital, reconocido en el art. 18.4 C.E., y cuya previsión en el ámbito laboral se recoge en el artículo 20 bis[39] del E.T., – el derecho a la intimidad en

---

responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información".

[37] A *sensu contrario* la STSJ del País Vasco núm. 482/2024, de 16 de enero. Trata un supuesto en el que las cámaras de videovigilancia captan a un trabajador de una empresa sustrayendo "dos bolsas con chatarra". El empleador del trabajador utiliza las grabaciones obtenidas para sustentar el despido. El Tribunal anula la prueba por entender que la empresa, a pesar de contar con la existencia de los dispositivos a los que nos venimos refiriendo, no ha cumplido con el deber de información del artículo 89.1 LOPD al no haber informado al trabajador que las cámaras podían usarse con este fin. El tribunal entiende que la excepción de "comisión de un acto ilícito" es transitoria, con el objetivo de dar una solución temporal hasta que las empresas regularicen el deber de información adicional en relación con los sistemas que la empresa utilizara y fueran previos a la entrada en vigor de la LOPD de diciembre de 2018. De no seguir esta línea, se estaría incentivando al empresario a proceder de forma irregular, no informando al trabajador, y amparándose en esas grabaciones para justificar eventuales despidos. Si bien, el TS, en Sentencia del 14 de enero núm. 23/2025, unifica doctrina en esta materia rechazando tal exigencia, reiterando que, en los casos de comisión de un acto flagrante ilícito, la existencia del cartel informativo en un lugar visible – *ex*. art. 22.4 LOPD – cumple con la regla requerida por el artículo 89 LOPD.

[38] GONZÁLEZ DEL RÍO, J.M., *El derecho a la intimidad del trabajador en el nuevo contexto laboral*. Tirant lo Blanch, Valencia, 2021.

[39] *"Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de*

relación con el entorno digital y a la desconexión –, y todo lo relativo al derecho a la protección de datos personales de la LOPD.

La STS núm. 489/2018, de 23 de octubre establece que: *"partiendo de la plurifuncionalidad de los datos que se almacenan en cualquier ordenador y otros dispositivos asimilables por su capacidad de acumular información vinculada a una persona (smartphone) se conviene en la necesidad de un tratamiento unitario a partir de la proclamación de un derecho al entorno digital. Sería un derecho de nueva generación que serviría para alumbrar y justificar distintos escalones de protección jurisdiccional."*. En cuanto a su extensión, el derecho comprendería *"toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos"*.

Por su parte, la Ley de Enjuiciamiento Criminal, dentro del capítulo denominado *"Registro de dispositivos de almacenamiento masivo de información",* hace alusión en el artículo 588 sexies a) al acceso a la información recogida en ordenadores, instrumentos de comunicación telefónica o telemática y otros dispositivos digitales de almacenamiento, exigiendo la necesidad de autorización judicial para acceder a los mismos. Ello implica que en el caso de que esos dispositivos hayan sido obtenidos como consecuencia, por ejemplo, de una entrada y registro en lugar cerrado (artículo 545 a 572 LECrim), la autorización para inspeccionar los dispositivos no puede considerarse implícitamente contenida en el auto que disponga la entrada y registro. Se requiere, pues, una resolución específica.

El Alto Tribunal, entre otras, en Sentencia núm. 489/2018, de 23 de octubre, concluye que *"la necesidad de esta autorización judicial (subsidiaria del consentimiento: si el afectado accede de forma libre, no hay cuestión) obedece a la consideración de estos instrumentos como esferas de almacenamiento de una serie compleja y densa de datos que afectan de modo muy variado a la intimidad del investigado (comunicaciones tuteladas por el art. 18 3° CE; contactos, fotografías, archivos personales, tuteladas por el art. 18 1° CE; datos personales y de geolocalización, que pueden cobijarse en el derecho a la protección de datos, art. 18 4° CE). La contemplación disgregada de cada una de esas realidades con regímenes de protección diferenciados resultaría ineficaz. Permitido, por ejemplo, el acceso directo de los agentes policiales a estos instrumentos para investigar datos únicamente protegidos por el derecho a la*

---

dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

intimidad (v.gr., los contactos incluidos en la agenda), no se podría acceder o consultar también otros datos tutelados por el derecho a la inviolabilidad de las comunicaciones albergados en el mismo dispositivo. El Legislador con buen criterio ha optado por otorgar un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando ese derecho constitucional de nueva generación, el derecho a la protección del propio entorno virtual".

Por todo lo anterior, y tal como sucede con injerencias en otros derechos, cualquier limitación en la investigación afectante al entorno digital requerirá, de no existir autorización judicial, el expreso consentimiento del trabajador, de ahí que vuelvan a resultar imprescindibles los protocolos de uso de herramientas informáticas y la correcta implantación de las medidas de control a las que ya se ha hecho referencia. [40]

3.3.5. Riesgos penales de la persona jurídica ante vulneraciones de estos derechos.

Como se ha expuesto en epígrafes anteriores, para garantizar el desarrollo de la actividad laboral de los trabajadores, el empresario implementa distintas medidas de control y dirección, y ante eventuales incumplimientos realiza averiguaciones por medio de investigaciones internas. No obstante, el desarrollo incorrecto de cualesquiera de estas puede generar responsabilidades penales para la persona jurídica, tal y como prevé el artículo 31 bis del Código Penal.

El abuso de estas facultades, cuando se traduce en actuaciones ilícitas como vigilancias desproporcionadas, acceso indebido a correos electrónicos, discriminación, acoso, etc., evidencia la necesidad de compatibilizar el ejercicio legítimo del poder empresarial con el respeto estricto a los derechos laborales, evitando así incurrir en conductas sancionables penalmente.

En el caso de las investigaciones internas, su ejecución por parte de la empresa constituye una *espada de doble filo*. Pese a que su finalidad mucha veces es atenuar o evitar la

[40] PASCUAL SUAÑA, O. Defensa de las personas jurídicas …. ob. cit. pp.144-146

responsabilidad penal, existen supuestos en los que, dado que estas indagaciones afectan severamente a derechos fundamentales, pueden ser constitutivas de delito.[41]

Destaca en estos términos y por su conexión con el supuesto de hecho, la STS núm. 328/2021, de 22 de abril [42], que confirmaba la condena de un empresario por un delito de revelación de secretos al haber accedido, en reiteradas ocasiones, al correo electrónico personal de un trabajador sin previamente haber excluido la expectativa de privacidad, con el objetivo de recopilar elementos de prueba para fundamentar su despido.

3.4. ILICITUD PRUEBA OBTENIDA POR PARTICULARES.

En los términos referidos y en relación a las pruebas obtenidas – o las que se pretenden obtener – para justificar el despido de un trabajador por las medidas de control y vigilancia adoptadas por el empresario, o por la posterior investigación empresarial, e incluso para iniciar un procedimiento judicial por los daños y perjuicios ocasionados por los actos del empleado, es necesario analizar la licitud de tal obtención. Por ello, es relevante hacer mención, tanto al denominado "*Caso Falciani*" como a las trascendentales sentencias dictadas sobre el asunto.

[41] NIETO MARTÍN, A., *"*Investigaciones internas*",* en NIETO MARTÍN, A., (Dir.), LASCURAÍN SÁNCHEZ, J.A., BLANCO CORDERO, I., PÉREZ FERNÁNDEZ, P., GARCÍA MORENO, B (Coords). *Manual de cumplimiento penal en la empresa*. Tirant lo Blanch, Valencia 2015, p. 242.

[42] Esta sentencia confirma la condena a un empresario que accedió reiteradamente y sin autorización al correo personal de un trabajador, utilizando información obtenida para fundamentar una querella, lo que supuso una vulneración del derecho al secreto de las comunicaciones protegido por el artículo 18.3 C.E.
El Tribunal confirmó la aplicación del artículo 197.1 del Código Penal, que sanciona el acceso no autorizado a documentos personales con el fin de descubrir secretos o vulnerar la intimidad. Argumentos como el error de prohibición o la legítima defensa fueron desestimados, ya que el empresario debía conocer la ilicitud de su conducta y no demostró una necesidad imperiosa que justificara la intromisión.
El Tribunal subrayó que, aunque el empresario tiene facultades de supervisión, estas no pueden vulnerar derechos fundamentales. El acceso al correo personal fue considerado desproporcionado y arbitrario al no existir, ni comunicación previa, ni medidas menos invasivas. Como consecuencia, el empresario fue condenado a un año de prisión y a la inhabilitación para el sufragio pasivo.

Esta materia gira en torno a las posibles fuentes de información susceptibles de constituir material probatorio en un proceso, y tuvo especial relevancia en nuestro país "*la sentencia Falciani*" dictada por el TS núm. 116/2017, de 23 de febrero.[43]

Históricamente, la doctrina española ha seguido la teoría de los frutos del árbol envenenado, limitando el uso de pruebas derivadas de una ilicitud original. Esta teoría, también denominada como teoría de la prueba prohibida, viene determinada en nuestro país por una evolución jurisprudencial marcada por la influencia estadounidense, pasando de declarar nula toda prueba obtenida vulnerando derechos fundamentales, sea de forma directa o indirecta – ilicitud que afecta a todo el proceso que gire en torno a la misma – a introducir ciertas excepciones que sí permiten tener en consideración dicha prueba.[44] Será posible esta circunstancia siempre que se lleve a cabo un análisis subjetivo de cada caso, ya que determinados derechos, por su carácter no absoluto, pueden sufrir limitaciones en atención al principio de proporcionalidad.

[43] La STS núm. 116/2017, de 23 de febrero, resuelve el recurso de casación interpuesto por el acusado contra la sentencia de la Audiencia Provincial de Madrid, que lo condenó por dos delitos fiscales. Los hechos se originan a raíz de la denominada *"Lista Falciani",* un conjunto de datos obtenidos de manera irregular por un exempleado del HSBC que revelaba información sobre cuentas bancarias en Suiza no declaradas a las autoridades fiscales españolas. La Agencia Tributaria recibió estos datos gracias a la cooperación internacional con las autoridades francesas, y detectó que el acusado poseía cuentas con activos significativos que no habían sido declarados, lo que motivó la investigación y posterior acusación por fraude fiscal.
Desde el punto de vista jurídico, el acusado alegó la ilicitud de la prueba, sosteniendo que la información obtenida vulneraba derechos fundamentales, en particular el derecho a la intimidad y el secreto bancario. En este sentido, el TS aborda la aplicabilidad del artículo 11 LOPJ, que regula la exclusión de pruebas obtenidas con vulneración de derechos fundamentales. Sin embargo, la Sala concluye que dicha información no está afectada por la regla de exclusión probatoria, dado que la prueba no fue obtenida por las autoridades españolas de manera directa ni a través de mecanismos que vulneraran derechos fundamentales, sino que llegó a la AEAT por vía de la cooperación internacional con Francia. Además, subraya que el particular que obtuvo los datos (Hervé Falciani) no actuó con la intención de prefabricar pruebas para un procedimiento penal, sino que su acción estuvo motivada por otros intereses ajenos a la investigación del delito.
La sentencia establece un precedente relevante en materia de valoración de pruebas obtenidas por particulares y su admisión en procesos penales, reafirmando que la ilicitud en el origen de una prueba no implica automáticamente su exclusión si no hay vulneración de derechos fundamentales por parte del Estado o si la prueba llega a las autoridades por cauces legales.

[44] La STC núm. 114/1984, de 29 de noviembre se plantea por primera vez el uso de pruebas que hayan vulnerado derechos fundamentales para dictar una sentencia condenatoria, debiendo ponderar los intereses en juego.

Como referimos, la regla general establece que cualquier prueba obtenida vulnerando derechos fundamentales así como las derivadas de estas son inadmisibles. Ahora bien, esta exclusión no es absoluta.

Un aspecto clave en la obtención de pruebas es la *"conexión de antijuridicidad"*[45], donde el TC entiende que, en realidad, se presupone que entre las pruebas obtenidas – derivadas incluidas – existe una conexión causal, pero exige más que una simple relación causal entre la prueba ilícita y la derivada de la misma. Para que la prueba derivada sea inadmisible debe existir un vínculo jurídico sustancial que prolongue la vulneración del derecho fundamental. Existen excepciones derivadas de la doctrina estadounidense, como la prueba jurídicamente independiente que es válida si no está conectada causalmente con la prueba ilícita; el descubrimiento inevitable que admite pruebas que se habrían obtenido legalmente en cualquier caso; y el hallazgo casual, aplicable cuando la prueba se encuentra de forma fortuita sin intención de vulnerar derechos.

En el caso de pruebas obtenidas por particulares, la jurisprudencia establece que su admisibilidad depende de la gravedad de la vulneración y del respeto al principio de proporcionalidad. Si bien, la regla de exclusión se aplica principalmente a actuaciones de autoridades públicas, puede extenderse a pruebas obtenidas ilícitamente por particulares si afectan gravemente a derechos fundamentales. En definitiva, es necesario un análisis casuístico para equilibrar la eficacia del proceso penal con la protección de los derechos fundamentales.[46]

---

[45] BARRANCO GÁMEZ, J.M. *Excepciones a la conexión de antijuridicidad para el Tribunal Constitucional.* Ilustre Colegio de Abogados de Huelva 2020 [En línea] http://www.icahuelva.es/wp-content/uploads/descargas/doctrinales/articulos-doctrinales-Excepciones-TC.pdf [consulta: 2 feb. 2024] Concepto definido por el citado autor como: *La conexión de antijuridicidad supone el establecimiento de un enlace jurídico entre una prueba y otra, de tal manera que, declarada la nulidad de la primera, se produce en la segunda una conexión que impide que pueda ser tenida en consideración por el Tribunal sentenciador a los efectos de enervar la presunción de inocencia del acusado. Pero esta conexión no es meramente causal sino que admite excepciones, que se traducen en la práctica en limitaciones de la prohibición absoluta de valoración de las pruebas indirectamente derivadas de una infracción constitucional. Es decir que para evitar extender hasta el infinito el efecto prohibitivo derivado del articulo 11.1 LOPJ, se admiten excepcionalmente factores de corrección. El Tribunal Constitucional español ha venido admitiendo excepciones que, alcanzan no solo a la eficacia refleja de la prueba ilícita sino a la propia aplicación directa de la regla de exclusión*" .

[46] PLANCHADELL GARGALLO, A., "Prohibiciones probatorias en la investigación de delitos cometidos por personas jurídicas." en GÓMEZ COLOMER, J.L.., (Dir.), MADRID BOQUÍN, C.M. (Coord.), *Tratado sobre compliance penal. Responsabilidad*

En relación con lo anterior, la mencionada STS núm. 116/2017, introdujo una excepción clave: si la prueba ha sido obtenida por un particular con absoluta desconexión de cualquier tipo de actividad estatal y sin intención de ser usada en un proceso judicial, puede ser admitida.

La STC núm. 97/2019, de 16 de julio [47] reafirmó la validez de la prueba obtenida en la *Lista Falciani*, pero con matices. En su análisis, distinguió entre la ilicitud del acto de obtención y su impacto procesal, concluyendo que no toda vulneración de un derecho fundamental conlleva la exclusión automática de la prueba. En el caso concreto, argumentó que no se comprometía la integridad del proceso ni se producía una desigualdad entre las partes.

En conclusión, las sentencias referidas provocan que la jurisprudencia española se incline hacia un enfoque más pragmático y utilitarista sobre la prueba ilícita, priorizando un análisis de ponderación sobre su impacto procesal y la necesidad de exclusión. Esta evolución tiene implicaciones significativas en el tratamiento de pruebas obtenidas por particulares, lo que podría influir en futuros casos relacionados con la privacidad, la protección de datos y el derecho penal económico.[48]

En el ámbito laboral, el análisis de la licitud de pruebas obtenidas por empresarios para controlar o sancionar a empleados sigue principios similares, pero con matices importantes.

---

penal de las personas jurídicas y modelos de organización y gestión. Tirant lo Blanch, Valencia, 2019, pp. 1121- 1140.

[47] Resuelve el recurso de amparo interpuesto por el condenado frente a la STS núm. 116/2017. El recurrente alegó que su condena se basó en pruebas obtenidas con vulneración de derechos fundamentales, en particular, su derecho a la intimidad y a un proceso con todas las garantías. El TC analiza la licitud de la prueba obtenida por un particular y concluye que el artículo 11.1 LOPJ establece la exclusión de pruebas obtenidas con vulneración de derechos fundamentales, pero su aplicación debe interpretarse de manera flexible y en función de cada caso. En este sentido, el Tribunal sostiene que la información utilizada por la Hacienda Pública provenía de autoridades francesas a través de mecanismos de cooperación internacional, lo que desvincula su obtención de cualquier injerencia estatal en la violación de derechos fundamentales. Además, argumenta que los datos fiscales obtenidos se referían a aspectos periféricos de la intimidad económica del recurrente y no revelaban hábitos de vida u otros elementos altamente protegidos por el derecho a la privacidad.
El fallo del TC confirma la validez de la prueba utilizada en el proceso penal. Argumenta que la exclusión de pruebas obtenidas ilícitamente no puede aplicarse de manera absoluta cuando se trata de información recabada por un particular sin vinculación con el Estado, especialmente si posteriormente ha sido introducida en el proceso penal por vías legales.

[48] ZARAGOZA TEJADA, J.I., GUTIÉRREZ AZANDA, D.A., "La exclusión de la prueba ilícita tras la sentencia del Tribunal Constitucional de 16 de julio de 2019 sobre la "Lista Falciani", *Revista Aranzadi de derecho y proceso penal,* nº56, 2019, pp. 209-222

Debido a lo anterior, las pruebas deben obtenerse siguiendo los principios de proporcionalidad y necesidad; y con una finalidad legítima, como es la prevención de conductas ilícitas y la protección de intereses de la empresa.

En este sentido, las sentencias relacionadas con el *Caso Falciani*, permiten extraer una lógica aplicable al ámbito laboral. Cuando un empresario actúa de forma independiente, y obtiene una prueba que afecta a derechos fundamentales, su validez dependerá de: si se han respetado principios de proporcionalidad, y de si la obtención estaba desvinculada de una intención de prefabricar pruebas.

3.5. VIDEOVIGILANCIA EN EL ENTORNO LABORAL.

Tal y como se ha referido en expositivos anteriores, el E.T. – *ex.* art. 20.3 – faculta al empresario a adoptar las medidas de vigilancia y control oportunas, permitiéndole verificar el cumplimiento de las obligaciones y deberes laborales de los trabajadores.

Este poder de dirección empresarial posibilita la vigilancia y el control de la actividad laboral por medio de cámaras de videovigilancia. No obstante, este derecho del empresario no es ilimitado, por lo que el ejercicio de cualquier medida derivada del mismo exige el cumplimiento de determinados deberes y garantías que giran esencialmente en la exigencia de información al trabajador. De este modo, el empleador puede tratar las imágenes obtenidas[49] a través de sistemas de videovigilancia para el ejercicio ese control, debiendo informar de las posibles medidas relativas al tratamiento y finalidad de las imágenes a los trabajadores con carácter previo, y de forma expresa, clara y concisa.[50]

Como se ha referido, una de las sentencias que supusieron un cambio paradigmático es la popularmente conocida como *«caso Bershka»*[51], dictada antes de la entrada en vigor de la

[49] El empleador cuenta con un plazo máximo de un mes desde su captación, en términos generales, para el tratamiento de las imágenes obtenidas, tal y como prevé el artículo 22.3 LOPD.

[50] «*Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo»*, previsto en el artículo 89.1 LOPD.

[51] STC núm. 39/2016, de 3 de marzo. El Tribunal Constitucional desestima el recurso de amparo presentado por una trabajadora de la empresa Bershka BSKA España, S.A., previamente despedida tras comprobar, por cámaras de videovigilancia instaladas en el lugar de trabajo, que había sustraído dinero de la caja.

LOPD. El fallo del Tribunal refuerza la facultad del empresario de utilizar la videovigilancia como medio de control laboral sin requerir el consentimiento expreso del trabajador, siempre que respete el deber de información y los principios de proporcionalidad. Además, legitima la utilización de grabaciones como prueba en procedimientos disciplinarios, consolidando su validez en el marco de la relación laboral.

Como se infiere de la meritada resolución, la grabación de los trabajadores en su puesto de trabajo es lícita y, por tanto, justificada cuando el empresario cumpla los requisitos que se desarrollarán a continuación:

3.5.1 Juicio de proporcionalidad.

En los términos a los que nos venimos refiriendo, y de acuerdo a la doctrina sentada por el TC[52], todas las medidas de vigilancia empresarial que pudieran vulnerar, o al menos restringir, derechos fundamentales de los trabajadores tienen que cumplir unas garantías, siendo en todo caso medidas adecuadas que superen el juicio de proporcionalidad: la medida ha de ser susceptible de conseguir el objetivo propuesto (*juicio de idoneidad*); tiene que ser necesaria, en el sentido de que no exista otra medida menos invasiva para la consecución de tal propósito con igual eficacia (*juicio de necesidad*); y, finalmente, la necesidad de ser ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (*juicio de proporcionalidad en sentido estricto*).

Concretamente, el departamento de seguridad de INDITEX detectó irregularidades en la caja donde prestaba servicios la trabajadora, por lo que encargaron a una empresa de seguridad la instalación de una cámara en ese punto concreto, pudiendo controlar el manejo de la caja.
La cámara se instaló sin comunicación expresa a los trabajadores, si bien, en el escaparate del establecimiento, siendo este un lugar visible, se colocó el distintivo informativo.
Ante estos hechos, el Tribunal consideró ajustada a derecho la actuación de la entidad, rechazando que tal actuación haya vulnerado el artículo 18 C.E., protector del derecho a la intimidad personal y a la propia imagen.
Los argumentos principales son la proporcionalidad y la justificación de la medida ante las sospechas razonables de actos ilícitos – apropiación de dinero – idónea para la finalidad pretendida por la empresa – verificar si algún trabajador cometía irregularidades –, necesaria – proporciona pruebas al respecto – y equilibrada – puesto que la captación de la cámara se dirige única y exclusivamente a la caja, no suponiendo una vulneración del derecho citado, además de la colocación de los distintivos informativos sobre la existencia de cámaras, lo que posibilitaba a la trabajadora ser conocedora de tal medida.

[52] Doctrina aplicada en Sentencias como la mencionada STC núm. 39/2016, de 3 de marzo y la STC núm. 119/2022 de 29 septiembre.

En relación con la cuestión planteada por RECAUCHUTADOS, tal y como se desprende de los antecedentes de hecho referidos en el epígrafe correspondiente, la entidad cumple *de facto* con estas garantías, y por si fuera poco, ha informado por partida doble a los trabajadores de la captación de imágenes por las cámaras de seguridad en el área de trabajo[53], tanto de forma individual mediante el clausulado incorporado en los contratos como de forma colectiva con la colocación de los carteles informativos pertinentes exigidos tras el «*caso Bershka*».

En supuestos como este último, en los que únicamente se informa a los trabajadores mediante la colocación de los dispositivos relativos a la "*zona controlada por videovigilancia*", no es necesaria información adicional que determine la finalidad de la recogida de los datos personales, puesto que, como establece la STS núm. 817/2021, de 21 de julio, cuando el trabajador conoce que se ha instalado un sistema de control por videovigilancia, no es obligado especificar la finalidad exacta que se le ha asignado a ese control, rebajando así las exigencias informativas para la empresa.[54]

A mayor abundamiento, y además del cumplimiento ya constatado, RECAUCHUTADOS no ha instalado las cámaras en lugares vedados por la normativa, como son los destinados al descanso o esparcimiento de los trabajadores, comedores, aseos o, en términos generales, todos aquellos de carácter reservado, en los que existiera una expectativa razonable de privacidad, sino que estaban instaladas, con sus correspondientes carteles, en todas las zonas de trabajo, incluida la zona de almacenamiento[55] donde se obtenía el material objeto

[53] STC núm. 29/2013, de 11 de febrero y STS núm. 1685/2013, de 13 de mayo.
[54] GARCÍA SALAS, A.I. *Videovigilancia laboral y cámaras de seguridad. A propósito de la STS de 21 de julio de 2021.* Criterios jurisprudenciales, Poder de dirección y vigilancia de la actividad laboral, Protección de datos, Videovigilancia. El Foro de Labos. 2021 [En línea]. https://www.elforodelabos.es/2021/10/videovigilancia-laboral-y-camaras-de-seguridad-a-proposito-de-la-sts-de-21-de-julio-de-2021/ [consulta: 18 nov. 2024]
[55] Tiene patentes similitudes con el supuesto tratado la STSJ núm. 4879/2024, de 23 de septiembre. En el caso allí enjuiciado se aborda el despido disciplinario de un trabajador por la sustracción de cobre de la zona de almacenamiento. La empresa utilizó las grabaciones captadas por cámaras de dicha zona para evidenciar el robo y justificar el consecuente despido disciplinario. La cuestión es que la empresa, tras detectar un consumo elevado de cobre que no se correspondía con la realidad fáctica, sospechaba de robos por parte de empleados, y decidió instalar cámaras en la zona de almacenaje. El Tribunal consideró que, a pesar de no haber aviso expreso en esta zona, la medida era idónea, necesaria, proporcionada y justificada, más si cabe, por la manifiesta visibilidad de las

del ilícito[56]. Por lo tanto, las cámaras no estaban instaladas de forma subrepticia, sino que estaban ubicadas en lugares visibles por cualquier persona que se encontrase en las instalaciones.

Cabe añadir, que las cámaras no fueron utilizadas por RECAUCHUTADOS para realizar una investigación de carácter prospectivo, sino que su instalación responde a cuestiones de seguridad laboral dentro del marco legal, y en este caso, para verificar la posible existencia de una conducta irregular, muy concreta, detectada en los días previos.

Con base en lo expuesto, se puede afirmar que la actuación empresarial de RECAUCHUTADOS analizada sí cumple con todos y cada uno de los requisitos y garantías exigidos por nuestros tribunales, siendo ajustada a derecho. No se puede considerar como desequilibrado el grado de intromisión en la esfera de la intimidad del trabajador – *ex*. art. 18.1 CE – , en términos de espacio y tiempo, frente a los derechos e intereses de la empresa en la detección y sanción de las conductas atentatorias contra la buena fe contractual, en el marco del ejercicio de los derechos de a la propiedad privada y a la libertad de empresa, reconocidos en los artículos 33 y 38 CE, respectivamente. [57]

3.5.2. Asunto López Ribalda.

En el contexto del ilícito consumado en las instalaciones de RECAUCHUTADOS y, en general, en todo lo relativo a la videovigilancia en el entorno laboral, es imprescindible la sentencia del asunto *«López Ribalda y otros contra España II»*[58], dictada el 17 de octubre de

---

cámaras instaladas en la sala de almacenaje y la ya presencia de cámaras debidamente señalizadas en otras zonas de las instalaciones.

[56] Art. 89.2 LOPD.

[57].HUERTA PÉREZ, L. *El despido acreditado por la captación de imágenes en un centro de trabajo sin haber informado previamente a los trabajadores es válido.* 2022 [En línea]. https://www.buadeslegal.com/el-despido-acreditado-por-la-captacion-de-imagenes-en-un-centro-de-trabajo-sin-haber-informado-previamente-los-trabajadores-es-valido/ [consulta 20 nov. 2024].

[58] Esta controversia tiene su origen en la captación de imágenes por las cámaras instaladas en un supermercado ante las pérdidas que este venía acumulando en los últimos meses, superando los 80.000 euros. Algunas de estas cámaras de videovigilancia fueron instaladas en lugares visibles con la correspondiente información a los trabajadores, mientras que otras tantas se colocaron de forma oculta sin notificación alguna a los empleados, ni a la representación de los trabajadores.

2019 por la Gran Sala del TEDH[59]; que refuerza más si cabe la decisión empresarial de RECAUCHUTADOS de optar, ante los hechos ya descritos, por un eventual despido disciplinario.

Este asunto, en el que la empleadora es una conocida empresa de supermercados, aborda una serie de despidos donde la entidad extinguió la relación laboral de los trabajadores por los hurtos cometidos en sus instalaciones, constatados por las cámaras de videovigilancia.

La sentencia dictada por la Gran Sala del TEDH tiene un gran impacto en el ámbito laboral puesto que permite a los empleadores la adopción de medidas de vigilancia más restrictivas en casos excepcionales, siempre que se respeten los requisitos de proporcionalidad, justificación y protección de la dignidad a los que ya había hecho, en gran parte, referencia nuestro Tribunal Constitucional – sentencias como la comentada STC núm. 39/2016, de 3 de marzo – reforzando su capacidad para actuar frente a los incumplimientos laborales.

En el asunto López Ribalda, el TEDH revisó las decisiones adoptadas por los tribunales españoles sobre los despidos disciplinarios y concluyó que, siendo estas correctas, habían logrado un equilibrio adecuado entre el derecho de las demandantes al respeto de su vida privada y el interés del empleador en salvaguardar sus derechos patrimoniales y garantizar el funcionamiento correcto de la empresa.

La Gran Sala del Tribunal de Estrasburgo consideró que la medida adoptada por la entidad es lícita. Las sospechas de robo y connivencia entre varios trabajadores legitima la captación de las imágenes, más si cabe, en la forma concreta en la que se produjeron (*espacio abierto,*

Las cámaras grabaron a varios empleados participando de algún modo en los ilícitos que se sospechaban y fueron despedidos, basándose en estas grabaciones, por incumplimiento grave de sus obligaciones laborales.
Los demandantes, que alegaron que la instalación de cámaras ocultas violó su derecho a la privacidad – art. 8 del Convenio Europeo de Derechos Humanos – y que las pruebas obtenidas eran inadmisibles, acudieron al Tribunal de Estrasburgo tras agotar las vías de recursos ante las jurisdicciones españolas, puesto que estos consideraban que tales grabaciones constituían un medio lícito de prueba. En un primer momento, el TDH falló a favor de los reclamantes, en su sentencia de 9 de enero de 2018, declarando que los órganos españoles no habían protegido adecuadamente el derecho a la intimidad de los trabajadores, para posteriormente, y en sentencia de 17 de octubre de 2019, justificar la licitud de la medida y la correcta actuación de los tribunales nacionales.
[59] ECLI:CE:ECHR:2019:1017JUD000187413.

accesible a todo el personal), limitando de este modo la intromisión en la privacidad de las demandantes y disminuyendo en consecuencia la expectativa de intimidad.

Además, la vigilancia fue temporal, desarrollándose durante un espacio de tiempo breve y limitado pero suficiente para identificar a los responsables de los robos.
Conforme se ha expuesto, este primer análisis no dista mucho de lo ya previsto por nuestro Alto Tribunal. Ahora bien, la especial relevancia de la sentencia del TEDH es la información al trabajador, en cualquiera de sus formas, en supuestos de videovigilancia encubierta[60]. En este caso, se justificó por la protección de intereses privados relevantes que justifican esta omisión de información, concretamente las sospechas razonables de graves irregularidades y las cuantiosas pérdidas económicas sufridas por la empresa.

Esta falta de información previa sobre las cámaras ocultas, contraria con carácter general a la normativa española de protección de datos, fue relativizada por la Gran Sala al argumentar que, en casos como el analizado, la protección de intereses legítimos puede justificar esta ausencia de notificación previa.[61]

La sentencia se enmarca en una línea jurisprudencial continuista sobre la protección de la vida privada de los trabajadores. El TEDH aplicó criterios ya establecidos en el «*caso Barbulescu*» – objeto de análisis en el siguiente epígrafe – relacionado con la vigilancia de las comunicaciones electrónicas laborales. Mientras que en aquel caso se destacó la importancia de notificar al trabajador, siendo la intrusión más intensa al acceder a contenidos privados, en *«López Ribalda»* se valoró la menor intromisión, al tratarse de grabaciones en espacios laborales abiertos y de una conducta atribuida más grave (robo frente al uso personal de recursos laborales) [62].

[60] No obstante, en algunas sentencias como la STC núm. 186/2000, de 10 de julio, nuestros tribunales les ya habían admitido prácticas empresariales sobre videovigilancia oculta en el contexto de un control extraordinario de los trabajadores una vez existían sospechas graves y fundadas.
[61] Esta decisión fue controvertida, como así da cuenta el voto particular conjunto de los jueces: De Gaetano, Yudkivska y Groez. Y es que, su percepción es que esta ausencia de información debería haber sido determinante en la evaluación de proporcionalidad, pudiendo la empresa haber recurrido a medidas menos intrusivas, como informar a la policía antes de optar por estas de iniciativa propia.
[62] CANO PALOMARES, G.. *Los derechos del trabajador ante el Tribunal de Estrasburgo (I): el caso López Ribalda y otros contra España o cómo un proceso de despido disciplinario de las trabajadoras de un supermercado llega a Estrasburgo*. 2020 [En línea]. https://www.idluam.org/blog/los-derechos-del-trabajador-ante-el-tribunal-de-estrasburgo-

3.6. ACCESO AL CORREO CORPORATIVO DEL INVESTIGADO.

3.6.1. Jurisprudencia nacional.

Aunque las grabaciones obtenidas, según se ha concluido *ut supra*, pueden ser empleadas por RECAUCHUTADOS para justificar el despido del trabajador, al objeto de asegurar la prosperabilidad de ese cese forzoso en la relación laboral, procede analizar la posibilidad de que la entidad acceda al email del empleado para obtener más elementos de cargo.

Esta posibilidad de control sobre las comunicaciones de los trabajadores mediante el acceso a su correo corporativo es otro aspecto relevante en el marco del poder de dirección y control de la actividad laboral por parte del empresario – mencionado art 20.3 ET –.

RECAUCHUTADOS se plantea acceder al correo electrónico corporativo del trabajador implicado en los ilícitos con el fin de obtener información acerca del destino del material sustraído. Ante esta cuestión, y a efectos de dar un correcto asesoramiento a la mercantil, deben observarse diferentes aspectos para determinar la idoneidad de la medida planteada:

En primer lugar, el precepto incorporado al E.T. por la disposición final 13 LOPD sobre los *"derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión"* en el uso de los dispositivos digitales puestos a su disposición por el empleador – *ex*. art. 20 bis E.T – y la relación que este guarda con el articulado de la propia LOPD.

Como ya se ha analizado, mediante el acceso al correo electrónico corporativo por parte del empleador se pueden ver afectados diferentes derechos fundamentales, por lo que se trata de una cuestión muy delicada. En tal sentido, para que la invasión sea lícita, el TS ha subrayado la necesidad de eliminar la expectativa de privacidad que pudiera tener el empleado[63]. Exclusión que exige, nuevamente, el cumplimiento de unos requisitos para que tal acceso sea lícito.

---

i-el-caso-lopez-ribalda-y-otros-contra-espana-o-como-un-proceso-de-despido-disciplinario-de-las-trabajadoras-de-un-supermercado-llega-a-e/ [consulta: 24 nov. 2024]

[63] Véase: derechos afectados por estas prácticas empresariales: a la intimidad personal – art. 18.1 C.E. –, al derecho al secreto de las comunicaciones – art. 18.3 C.E. – y al entorno digital – art. 18.4 C.E. – .

Tomando como referencia la Sentencia del Tribunal Supremo núm. 489/2018, de 23 de octubre, resuelve esta diatriba en los siguientes términos:

"allí donde exista acuerdo expreso de fiscalización se estará excluyendo toda expectativa de privacidad. Pero la exclusión de esa expectativa ha de ser expresa y consciente, sin que pueda equipararse a ésta una pretendida renuncia derivada de la voluntad presunta del trabajador".

De este modo, se exige informar al trabajador de forma expresa de la utilidad del correo electrónico corporativo; de que se trata de una herramienta susceptible de control o monitorización por parte de la empresa y; de que, en supuestos como el presente, tiene uso exclusivamente profesional, no debiendo emplearse con fines personales.

En todo caso, la información se le debe hacer llegar al trabajador en cualquier momento de la relación laboral – siempre con anterioridad a la vigilancia, monitorización o acceso –, idealmente al comienzo de ésta incorporándola al contrato de trabajo, y debe acreditarse su recepción de forma fehaciente, por ejemplo, mediante la firma del trabajador.

Al respecto, según la STS (Sala de lo Penal) núm. 328/2021, de 22 de abril (F.D. 3.9). "*empresario y trabajador pueden fijar los criterios de ese control, pactando la renuncia, no ya a la intimidad, sino a la propia inviolabilidad de las comunicaciones. Y allí, donde exista acuerdo expreso sobre fiscalización, se estará excluyendo la expectativa de privacidad que, incluso en el ámbito laboral, acompaña a cualquier empleado".*

Estos criterios deben de respetar los estándares mínimos de protección de la intimidad de los trabajadores, de conformidad con los usos sociales y los derechos reconocidos constitucionalmente, siendo necesaria la participación de los representantes legales de los trabajadores en ese proceso de elaboración de los términos y normas sobre uso de equipos informáticos y correos corporativos, como así recoge el artículo 87.3 LOPD.

A estos efectos, los tribunales van a considerar irrelevante que los contratos de trabajo determinen expresamente los criterios de uso establecidos por los empleadores acerca del uso de los dispositivos digitales, si estos no han sido negociados previamente con los representantes de los trabajadores – RLT – [64].

[64] Sobre la necesaria negociación, la SAN (Sala de lo Social), número 114/2022 de 22 de julio analizó un supuesto relativo a una política empresarial sobre el uso de medios digitales en el entorno laboral que incluía la posibilidad de conectar los ordenadores de la oficina

En este tipo de situaciones entran en juego los preceptos de nuestro ordenamiento que venimos mencionando, poder de vigilancia y control empresarial sobre la actividad laboral de sus trabajadores – *ex*. art. 20.3 E.T –, y las exigencias del derecho a la intimidad y el uso de los dispositivos digitales en el ámbito laboral – *ex*. art. 87.3 LOPD –, que sí bien están relacionados, pueden obedecer a realidades distintas.

Sigue este razonamiento la Sentencia del Tribunal Supremo 225/2024, de 6 de febrero, primero en relación con el artículo 20.3 E.T., indicando que:

"el precepto estatuario reconoce la facultad laboral para adoptar las medidas que estime más oportunas de vigilancia y control. Se trata de un precepto de carácter general aplicable a todo tipo de actividad, con independencia de los medios materiales que se utilicen para la realización del trabajo".

Respecto del artículo 87.3 LOPD, ya del propio precepto se desprende su carácter imperativo en los supuestos en los que el trabajo se realice mediante dispositivos digitales, al determinar este que los empresarios deberán establecer criterios de utilización y deberán participar en los mismos los representantes legales de los trabajadores. Al respecto añade el Tribunal que este artículo:

"se refiere específicamente a los criterios de utilización de los dispositivos digitales que el empresario pone a disposición de los empleados para la realización del trabajo, y al respecto, faculta al empresario para establecer normas y criterios para la utilización de los mismos, a la vez que establece limitaciones a ese poder de especificación empresarial vinculadas al derecho a la intimidad de los trabajadores. Sobre estas cuestiones específicas, la norma ordena que la elaboración de los criterios de utilización de dichos medios se realice con la participación de la RLT. Desde esa perspectiva, el art. 87.3 LOPD resulta una especificación, para un ámbito determinado, del genérico poder de dirección del artículo 20.3 ET, que legalmente ese explica porque en tal ámbito, la intimidad del trabajador resulta especialmente sensible. De ahí que el nuevo artículo 20 bis ET disponga que "Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión

---

cuando los empleados teletrabajaban, permitiendo una vigilancia en tiempo real de sus actividades. Pese a que estos criterios eran conocidos por los trabajadores e incluidos en el clausulado de cada contrato de trabajo individual, la sentencia declaró nula la instrucción emitida por la empresa sobre el uso de equipos informáticos y correos corporativos, y enfatizó que, aunque los contratos de trabajo especificaran que los dispositivos digitales debían utilizarse exclusivamente con fines profesionales, ello no eximía a la empresa de la obligación de negociar estas políticas con la representación legal de los trabajadores.

digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos".[65]

Con base en todo lo anterior, el Tribunal ha estimado que la no participación de la RLT conlleva la nulidad de las políticas de uso de los dispositivos, lo que implica que éstas no serían válidas, como tampoco lo sería su comunicación a los trabajadores. Y en relación con la sentencia concreta, indica que en virtud del carácter imperativo del artículo 87.3 LOPD, cualquier modificación de los criterios de utilización de los dispositivos digitales previamente establecidos, o actualización de los mismos que ya venían rigiendo en la empresa y que, consecuentemente, debieron ser elaborados cumpliendo la normativa vigente, deben ser fijados, nuevamente, con la participación de los representantes de los trabajadores.

3.6.2 Test Barbulescu

La sentencia de la Gran Sala del TEDH núm. 2017/61 de 5 de septiembre[66], en el conocido como caso *«Barbulescu contra Rumanía»*[67], sentó un precedente relevante en el acceso a los correos electrónicos corporativos de los trabajadores.

Este asunto, que aborda el despido de un trabajador, fue sustentado en que había utilizado la mensajería instalada en su ordenador para fines personales. Es fundamental destacar que

[65] STS núm. 225/2024 de 6 Feb. 2024, F.D. Tercero.
[66] ECLI:CE:ECHR:2017:0905JUD006149608.
[67] La controversia tiene su origen en una demanda presentada por un ciudadano rumano frente a Rumanía en virtud del artículo 34 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales en relación con el artículo 8 del Convenio Europeo de Derechos Humanos. El demandante trabajaba en una empresa como ingeniero de ventas, y a petición de su empresa creó una cuenta de mensajería en línea para una comunicación eficiente con los clientes. El reglamento interno de la empresa prohibía la utilización de los ordenadores con fines personales, pero no preveía la posibilidad de que la empresa vigilase la comunicaciones de los empleados.
En estos términos, la empresa supervisó sus conversaciones en la cuenta de mensajería, y tras comprobar que había intercambiado mensajes con su hermano y su novia, fue despedido.
El actor reclamó ante los tribunales nacionales rumanos, los cuales confirmaron el despido por parte de la empresa. No conforme, el demandante eleva su queja ante el TEDH, recibiendo nuevamente una respuesta negativa al considerar que la acción empresarial se trataba de un mero ejercicio del poder de dirección y de control de la actividad de los trabajadores. Finalmente el demandante solicita la remisión del asunto a la Gran Sala del Tribunal, la cual dicta sentencia favorable a sus intereses el día 5 de septiembre de 2017.

el trabajador había sido informado de las reglas generales contra el uso personal de los recursos empresariales, pero no había sido advertido específicamente sobre la posibilidad de que su ordenador fuese monitoreado.

La Gran Sala concluyó que, aunque los empleadores puedan supervisar comunicaciones en el trabajo, este monitoreo debe ser proporcional, transparente y ajustarse a la intensidad del control del empresario, estando los trabajadores advertidos de forma clara, aspectos que no se cumplieron en el *«caso Barbulescu»*. Adopta, por tanto, una postura más intervencionista y garantista, estableciendo criterios que se han implantado en el conocido como "test Barbulescu" necesario en los supuestos controvertidos de videovigilancia de las comunicaciones.

En consecuencia, se ha convertido en un referente obligatorio de los casos de vigilancia de comunicaciones electrónicas, ya sea mediante correo electrónico o mensajería instantánea en el entorno laboral. Sin embargo, y en relación con el epígrafe anterior, este test también es aplicable a cualquier forma de vigilancia electrónica o informática, incluida la videovigilancia.

En virtud de la doctrina Barbulescu, los Tribunales deben examinar una serie de parámetros:

En primer lugar, el conocimiento de la posible monitorización por el trabajador**.** Es fundamental verificar si el empleado fue informado previamente de la posibilidad de que el empleador adoptara medidas de control sobre su correspondencia u otras comunicaciones, y cual sería el uso de las mismas. La información proporcionada debe ser previa, clara, precisa, transparente y específica, conociendo igualmente cual serían las consecuencias en caso de un uso inapropiado por el trabajador. No basta con la existencia de protocolos internos que prohíban el uso de recursos técnicos para fines personales; también es necesario que la empresa informe explícitamente sobre los controles que se podrían realizar y los métodos empleados. Asimismo, esta cuestión debe cumplir con el principio de idoneidad, determinando el alcance de la vigilancia y el grado de intromisión en la vida privada del trabajador.

En segundo lugar, el test de proporcionalidad, referido a la legitimidad del empresario para adoptar tal medida y a la posibilidad de emplear alternativas menos intrusivas. El control debe superar este análisis, lo que implica que el empleador debe justificar un motivo legítimo para la vigilancia de las comunicaciones, especialmente cuando se accede a su contenido, lo que requiere una justificación más sólida. Esto incluye evaluar si el objetivo del empleador podría haberse alcanzado sin dicha intromisión, las consecuencias para el trabajador y la utilidad de la medida en relación con los fines perseguidos, además de garantizar que el trabajador contara con las debidas protecciones.[68]

4. CONCLUSIONES

Una vez analizado el supuesto de hecho, los derechos de las partes de la relación laboral, y la doctrina y jurisprudencia aplicable a situaciones como la detallada, hay que proporcionar un asesoramiento jurídico a la entidad dando contestación a los cuestiones planteadas ante nuestro servicio jurídico.

En primer lugar, respecto al acceso por parte de RECAUCHUTADOS al correo corporativo del trabajador para buscar acreditar, más si cabe, la comisión de los ilícitos objeto de investigación, hay que tener en cuenta, además de lo referido durante los ordinales anteriores – especial atención a la doctrina "Barbulescu" – lo previsto en la STS núm. 225/2024 de 6 febrero. En atención a la misma, es fundamental indicar que el trabajador no ha sido advertido por la mercantil sobre la posibilidad de que se adopten medidas de control sobre su correspondencia, o que directamente su equipo sea monitoreado. A causa de lo antedicho, parece evidente que el acceso al e-mail del trabajador por parte del empresario, bajo estas circunstancias, se realizaría sin excluir la expectativa de privacidad del Sr. Becerro, vulnerando así su derecho a la intimidad y al secreto de las comunicaciones. En consecuencia, las pruebas obtenidas serían ilícitas, y por tanto, devendrían nulas.

[68] FELIPE D. JIMÉNEZ, A. *El caso Barbulescu y su Impacto en la Jurisprudencia Constitucional*. [En línea] https://revistaconsinter.com/index.php/ojs/0710#_ftnref10 [consulta: 25 nov. 2024]

A mayor abundamiento, esta intervención difícilmente superaría el test de proporcionalidad analizado, pues, dados los hechos, es altamente probable que con esa injerencia no se obtengan nuevos elementos de comprobación respecto a los ya investigados.

En este sentido, para realizar esta intervención de forma correcta en futuras ocasiones y no infringir la normativa, los empresarios deben cumplir fundamentalmente con dos obligaciones:

- Excluir la expectativa de privacidad del trabajador: informándole siempre con anterioridad a la vigilancia del correo que se trata de una herramienta facilitada por la empresa con fines exclusivamente profesionales, y que podrá ser controlado y monitorizado.[69]
- Elaborar un procedimiento interno respecto al uso de las herramientas tecnológicas. Además, deberá indicar expresamente el protocolo de bloqueo de la cuenta de correo corporativa y su posterior gestión en caso de dimisión o despido. En este sentido, la LOPD matiza que la elaboración de estas políticas debe participar la representación legal de los trabajadores.

En segundo lugar, respecto a las imágenes obtenidas por las cámaras de seguridad y su uso para justificar el despido del trabajador, queda acreditado que la mercantil ha cumplido con todos los criterios establecidos, tanto por la normativa como por la jurisprudencia. Y es que, la entidad ha informado previamente al trabajador sobre la instalación y uso de los sistemas de videovigilancia, las cámaras se encuentran ubicadas de forma visible en zonas permitidas por la normativa, y únicamente se acude a las imágenes ante las sospechas de la comisión de ilícitos. Por lo que la actuación de la empresa resulta ajustada a derecho, proporcional y necesaria para con el objetivo perseguido, no pudiendo optar por medios de obtención de prueba distintos. [70]

En tercer lugar, y en relación con los ilícitos cometidos por el trabajador y acreditados por las pruebas videográficas, una vez probada la licitud de las mismas, sí se puede proceder a la extinción de la relación laboral del Sr. Becerro.

---

[69] STS núm. 489/2018, de 23 de octubre.
[70] Unificación de doctrina sobre la videovigilancia. Por todas, la ya referida STS núm. 23/2015, de 14 de enero.

El Convenio colectivo aplicable a la actividad empresarial de RECAUCHUTADOS prevé este tipo de actos como infracciones muy graves cuya sanción máxima aplicable es el despido del trabajador. Supuestos como el presente, están relacionados con el artículo 54, apartados 1 y 2.d) E.T., ya que se trata de un incumplimiento grave y culpable del trabajador que comete un hurto frente a otro compañero y frente a la empresa[71], constituyendo una transgresión de la buena fe contractual y abuso de confianza.

Por último, en caso de despido disciplinario, por las causas que aquí se han debatido, es preciso informar a la empresa de la necesidad de cumplir con unos requisitos formales que garanticen la eficacia de tal decisión. Las entidades tienen que entregar carta de despido por escrito al trabajador sancionado, y esta debe de contener los motivos por los que se adopta tal situación y la fecha en que tendrá efectos.[72] Ahora bien, además de estos dos requisitos, la STS núm. 1250/2024, de 18 de noviembre[73] incorpora un tercero, estableciendo la obligación de otorgar a la persona trabajadora una audiencia previa al despido.

En consecuencia, RECAUCHUTADOS debe otorgar esta audiencia previa al despido al Sr. Becerro para que pueda alegar lo que considere oportuno ante las acusaciones empresariales. Asimismo, es fundamental que la entidad documente adecuadamente la

[71] Siguiendo la línea marcada por el TS – por todas, STS núm. 750/2023 de 17 de octubre – , la sustracción de objetos en el ámbito laboral es encuadrable dentro de las causas de despido disciplinario consistente en la transgresión de la buena fe contractual. La sentencia citada, tilda estas conductas como merecedoras de la máxima sanción laboral, independientemente del valor de lo sustraído, puesto que lo importante no es el valor o el perjuicio económico que se causa a la empresa, sino la ruptura de la confianza que el empresario depositó en el trabajador.

[72] Previsión recogida en el artículo 55.1 E.T. En caso de ajustarse a estos requisitos, el apartado 4 del propio precepto establece que el despido será calificado como improcedente.

[73] La histórica STS núm. 1.250/2024, basada en el argumento del artículo 7 del Convenio 158 OIT, ratificado por España el 18 de febrero de 1985, de 18 de noviembre de 2024, establece la obligación de dar al trabajador la oportunidad de una audiencia previa antes de ser despedido disciplinariamente y poder hacer alegaciones al respecto, salvo que esto sea imposible (el propio artículo 7 indica que *"a menos que no pueda pedirse razonablemente al empleador que le conceda esta posibilidad";* algo que puede referirse a situaciones de fuerza mayor o situaciones excepcionales justificadas). Esta audiencia previa hay que diferenciarla con el exp. Contradictorio previsto en el artículo 55 E.T. en relación con el artículo 114 LRJS. En la actualidad, esta audiencia se hará con independencia de estar o no afiliado a un sindicato, y ser o no RLT, es decir, a todos los trabajadores.. A mayor abundamiento, la OIT no hace referencia al cumplimiento de un plazo predeterminado para la realización de la audiencia previa al despido, ni tampoco de los requisitos formales que ha de seguir. Por lo que, a falta de regulación normativa, serán los convenios o los propios tribunales los que definan estas condiciones.

realización de la misma, para garantizar que el trabajador ha tenido la posibilidad real de defenderse, cumpliendo así, plenamente, con este requisito.

5. BIBLIOGRAFÍA

BACIGALUPO, E., "Problemas penales del control de ordenadores del personal de una empresa", *Diario La Ley*, nº 8031, Sección Doctrina, 26 de febrero de 2013, Año XXXIV, Ref. D-79.

GALLARDO MOYA, R. "Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5 de septiembre de 2017 en el caso Barbulescu c. Rumania". Análisis de Jurisprudencia. *Revista de derecho social 79* Bomarzo, Albacete, 2017.

GONZÁLEZ DEL RÍO, J.M. *El derecho a la intimidad del trabajador en el nuevo contexto laboral*. Tirant lo Blanch, Valencia, 2021.

LÓPEZ AHUMADA, CHARRUTTI GARCÉN, M.L., JIMENEZ MARTÍNEZ, M.V., ROLDÁN MARTINEZ *La garantía de los derechos digitales en el ámbito laboral: políticas empresariales, ejercicio de derechos y límites al poder de control del trabajo,* Aranzadi, Navarra. 2023.

MARTÍN VALVERDE, A., RODRÍGUEZ-SAÑUDO GUTIÉRREZ, F., GARCÍA MURCIA, J. *Derecho del Trabajo,* 29º edición, Tecnos, Madrid, 2020.

NIETO MARTÍN, A., LASCURAÍN SÁNCHEZ, J.A., BLANCO CORDERO, I., PÉREZ FERNÁNDEZ, P., GARCÍA MORENO, B. *Manual de cumplimiento penal en la empresa*, Valencia: Tirant lo Blanch.

PASCUAL SUAÑA, O., *Defensa de las personas jurídicas en el proceso penal español. Especial referencia a los informes periciales de compliance,* Tirant lo Blanch, Valencia.

PASCUAL SUAÑA, O., "Mejores prácticas en los canales de denuncias", *Revista Brasileira de Direito Processual Penal,* Vol. 9, Nº. 2, 2023, págs. 575-607 (Vista do Mejores prácticas en los canales de denuncias)

PLANCHADELL GARGALLO, A., "Prohibiciones probatorias en la investigación de delitos cometidos por personas jurídicas." en GÓMEZ COLOMER, J.L.., (Dir.), MADRID BOQUÍN, C.M. (Coord.), *Tratado sobre compliance penal. Responsabilidad penal de las personas jurídicas y modelos de organización y gestión*, Valencia: Tirant lo Blanch, 2019.

RODRIGUEZ ESCANCIANO, S. *"*Videovigilancia de seguridad como prueba de ilícitos laborales ante sospecha de comportamiento irregular*", Revista de Jurisprudencia Laboral.* Número 10/2022.

ZARAGOZA TEJADA, J.I., GUTIÉRREZ AZANDA, D.A., "La exclusión de la prueba ilícita tras la sentencia del Tribunal Constitucional de 16 de julio de 2019 sobre la "Lista Falciani", *Revista Aranzadi de derecho y proceso penal,* nº56, 2019,

6. JURISPRUDENCIA

Sentencia del Tribunal Europeo de Derechos Humanos, Gran Sala en el caso Barbulescu v. Rumanía de 5 de septiembre de 2017.

Sentencia del Tribunal Europeo de Derechos Humanos, Gran Sala en el asunto López Ribalda y otros contra España, de 17 de octubre de 2019.

Sentencia del Tribunal Constitucional núm. 114/1984, de 29 de noviembre (Rec. 167/1984).

Sentencia del Tribunal Constitucional núm. 98/2000, de 10 de abril (Rec. 73/2000).

Sentencia del Tribunal Constitucional núm. 186/2000, de 10 de julio (Rec. 2662/1997).

Sentencia del Tribunal Constitucional núm. 70/2002, de 3 de abril (Rec. 3787/2001).

Sentencia del Tribunal Constitucional núm. 151/2004, de 20 de septiembre (Rec. 3660/2002).

Sentencia del Tribunal Constitucional núm. 77/2009, de 23 de marzo (Rec. 6970/2006).

Sentencia del Tribunal Constitucional núm. 29/2013, de 11 de febrero (Rec. 10522/2009).

Sentencia del Tribunal Constitucional núm. 39/2016, de 3 de marzo (Rec. 7222-2013).

Sentencia del Tribunal Constitucional núm. 97/2019, de 16 de julio (Rec. 1805/2017).

Sentencia del Tribunal Constitucional núm. 119/2022, de 29 de septiembre (Rec. 7211/2021).

Sentencia del Tribunal Supremo núm. 966/2006, de 26 de septiembre (Rec. 966/2006)

Sentencia del Tribunal Supremo núm. 1685/2013, de 13 de mayo (Rec. 1685/2013).

Sentencia del Tribunal Supremo núm. 116/2017, de 23 de febrero (Rec. 1281/2016).

Sentencia del Tribunal Supremo núm. 489/2018, de 23 de octubre (Rec. 1674/2017).

Sentencia del Tribunal Supremo núm. 338/2019, de 3 de julio (Rec. 803/2018).

Sentencia del Tribunal Supremo núm. 328/2021, de 22 de abril (Rec. 715/2020).

Sentencia del Tribunal Supremo núm. 225/2024, de 6 febrero (Rec. 263/2022).

Sentencia del Tribunal Supremo núm. 750/2023, de 17 de octubre (Rec. 5073/2022).

Sentencia del Tribunal Supremo núm. 1.250/2024, de 18 de noviembre (Rec. 4735/2023).

Sentencia del Tribunal Supremo núm. 23/2015, de 14 de enero (Rec. 5248/2023).

Sentencia de la Audiencia Nacional, Sala de lo Social, núm. 114/2022, de 22 julio (Rec. 178/2022).

Sentencia del Tribunal Superior de Justicia de Cataluña núm. 4879/2024, de 23 de septiembre (Rec. 1581/2024).

Sentencia del Tribunal Superior de Justicia del País Vasco núm. 482/2024, de 16 de enero (Rec. 2305/2023).

7. NORMATIVA

Constitución Española, de 27 de diciembre. «BOE» núm. 311 (1978)

Convenio Europeo de Derechos Humanos. (1950).

Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

Ley Orgánica 3/2018, 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. «BOE» núm. 294 (2018).

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. «BOE» núm. 157 (1985),

Ley Orgánica 10/1995, de 23 de noviembre del Código Penal. «BOE» núm. 281 (1995)

Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. «BOE» núm. 44 (2023)

Real Decreto Legislativo de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. «Gaceta de Madrid» núm. 260 (1882).

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. «BOE» núm. 255 (2015).

8. WEBGRAFÍA

www.avqlegal.com/es-posible-acceder-a-la-cuenta-de-correo-corporativo-de-un-trabajador-despedido/

www.bibliotecacompliance.com/wp-content/uploads/2021/02/FASC-2_INVESTIGACIONES-INTERNASpdf.pdf

www.buadeslegal.com/el-despido-acreditado-por-la-captacion-de-imagenes-en-un-centro-de-trabajo-sin-haber-informado-previamente-los-trabajadores-es-valido/

www.eduardorojotorrecilla.es/2017/09/de-barbulescu-i-barbulescu-ii-la-gran.html

www.elforodelabos.es/2021/10/videovigilancia-laboral-y-camaras-de-seguridad-a-proposito-de-la-sts-de-21-de-julio-de-2021/

www.has.es/2020/12/01/el-ts-cierra-el-circulo-lopez-ribalda-ii-validez-de-la-instalacion-de-camaras-ocultas-en-empresas-videovigilancia/

www.icahuelva.es/wp-content/uploads/descargas/doctrinales/articulos-doctrinales-Excepciones-TC.pdf

www.idluam.org/blog/los-derechos-del-trabajador-ante-el-tribunal-de-estrasburgo-i-el-caso-lopez-ribalda-y-otros-contra-espana-o-como-un-proceso-de-despido-disciplinario-de-las-trabajadoras-de-un-supermercado-llega-a-e/

www.legacy.acfe.com/report-to-the-nations/2024/

www.protecciondatos-lopd.com/empresas/compliance/canal-denuncias/procedimiento/#Como_debe_ser_el_procedimiento_del_canal_de_denuncias_de_una_empresa

www.revistaconsinter.com/index.php/ojs/0710 - _ftnref10