

EL DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO LABORAL

THE RIGHT TO PRIVACY AND TO THE PROTECTION OF PERSONAL DATA IN THE WORKPLACE

Antonio Felipe Delgado Jiménez¹ – <https://orcid.org/0000-0002-1620-2737>

Resumen

Se analiza la función equilibradora, entre trabajador y empresario, de los derechos fundamentales en el ámbito de la relación laboral, al tiempo que se hace hincapié en que el derecho a la intimidad no es un derecho ilimitado, sino que puede ceder ante otros derechos constitucionales. Asimismo, se estudia el derecho a la protección de datos personales – distinguiéndolo del derecho a la intimidad personal – que tiene por objeto garantizar la libertad del individuo en relación a su autodeterminación respecto del tratamiento de sus datos personales por terceros.

Palabras clave: Derecho a la intimidad; Derecho al secreto de las comunicaciones; Derecho a la protección de datos personales en el ámbito laboral.

Abstract

The balancing function, between worker and employer, of the fundamental rights in the field of the labor relationship is analyzed, while emphasizing that the right to privacy is not an unlimited right, but that it can yield to other constitutional rights. Likewise, the right to the protection of personal data is studied – distinguishing it from the right to personal privacy – which aims to guarantee the freedom of the individual in relation to their self-determination regarding the processing of their personal data by third parties.

Keywords: Right to privacy; Right to secrecy of communications; Right to the protection of personal data in the workplace.

Sumario: 1. Introducción; 2. El derecho a la intimidad; 2.1. Control del ordenador y derechos fundamentales del trabajador; 2.1.1. Existencia de expectativa razonable de privacidad; 2.1.2. El acceso a contenidos privados mediando consentimiento del trabajador afectado; 3. El derecho a la protección de datos personales; 3.1. Su autonomía frente al derecho a la intimidad; 3.2. Sus diferencias respecto al derecho a la intimidad; 3.3. Afectación del derecho a la protección de datos personales; 4. Conclusiones; Bibliografía.

Recibido/Received 10.04.2021 – Aprobado/Approved 09.11.2021

¹ Doctor en Derecho Universidad Complutense de Madrid. E-mail: antdelga@ucm.es.

1 INTRODUCCIÓN.

La implantación de las TIC en las organizaciones empresariales ha determinado una radical transformación de la prestación laboral tradicional que, si bien ha supuesto indudables avances desde el punto de vista de la eficiencia productiva y el ahorro de costes, también ha determinado la acumulación de una enorme batería de datos que, adecuadamente tratados, suponen la obtención de una radiografía, no solo de la actividad laboral *stricto sensu*, sino de la persona del trabajador.

De modo paralelo se ha venido operando un proceso de fortalecimiento del poder empresarial vinculado a la implantación de las TIC en las empresas cuyo impacto se ha dejado notar especialmente respecto de los derechos fundamentales del trabajador, lo que exige retomar el debate sobre los derechos fundamentales en el ámbito del contrato de trabajo y sus relaciones con respecto al poder de dirección y control del empresario.

Partiendo de las anteriores premisas, el objetivo del presente trabajo consiste en analizar la problemática que conlleva el control tecnológico de la actividad laboral por parte del empresario y sus implicaciones respecto a los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales, para lo cual habrá que individualizar en primer lugar los derechos en juego; analizar, acto seguido, su regulación legal (si existiere) para, finalmente, escudriñar la doctrina jurisprudencial sobre el tema en cuestión al objeto de extraer las conclusiones pertinentes.

Para alcanzar el objetivo señalado se ha dividido este artículo en dos capítulos, cada uno de los cuales responde a una pregunta objeto de investigación, a saber:

- a) el análisis del derecho a la intimidad;
- b) el estudio del derecho a la protección de datos personales.

Con independencia de las conclusiones generales obtenidas con el presente estudio, las cuales figuran al final de la obra, sí podemos adelantar que una de las principales conclusiones extraídas del presente trabajo ha sido que la vida social privada del trabajador en el seno de las empresas no puede en ningún caso reducirse a cero, teniendo el Estado la obligación positiva (obligación de hacer) de procurar que se respete la vida privada de los empleados en el seno de las organizaciones empresariales, debiendo el legislador cumplir con esa obligación positiva mediante la fijación del marco normativo adecuado que determine la protección de los diversos intereses en juego y, en defecto de regulación legal, corresponderá a los órganos judiciales nacionales asegurar que la adopción empresarial de medidas de vigilancia de la correspondencia y de otras comunicaciones se efectúe con las garantías adecuadas y suficientes contra los abusos y las arbitrariedades.

2 EL DERECHO A LA INTIMIDAD.

El análisis de la intimidad en el seno de las relaciones laborales ha de partir de un hecho evidente, cual es que la Constitución no se detiene a las puertas de la

empresa habida cuenta de que los derechos fundamentales no pueden ser ignorados por el clausulado de un contrato de trabajo², ejerciendo los derechos fundamentales en el ámbito de la relación laboral una función equilibradora entre trabajador y empresario³ dada la evidente asimetría de dicha relación⁴, pudiendo quedar damnificado el derecho a la intimidad en numerosas ocasiones y momentos que se producen en los centros de trabajo como, por ejemplo, con motivo de la instalación de instrumentos de audición o de un circuito cerrado de televisión⁵ o con ocasión de la puesta en marcha de cámaras de control de acceso al lugar de trabajo⁶ o mediante el control del correo electrónico⁷, etc., siendo así que los derechos fundamentales del trabajador adquieren especial relevancia en un ámbito como el laboral en el que el poder de dirección del empresario puede entrar en colisión con aquellos.

En efecto, de conformidad con lo dispuesto en el art. 20.3 ET “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 humana...” y, de acuerdo con el art. 20 bis ET, “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 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”, siendo evidente que la implementación de tales medidas por parte del empleador no puede hacerse ignorando que la otra parte del contrato de trabajo también es titular de derechos fundamentales⁸, de forma que la eficacia de estos en las relaciones jurídicas interprivatos proyecta sobre el contrato de trabajo un elemento heterónomo que opera de forma prevalente sobre las obligaciones contraídas por las partes haciendo que la empresa no sea una fortaleza inexpugnable frente a los valores y derechos constitucionales⁹, de modo que el extraordinario avance que supone el progreso de las nuevas tecnologías no puede convertirse en un

² STC 88/1985, de 19 de julio, FJ 2º.

³ STC 129/1989, de 17 de julio, FJ 5º.

⁴ MIERES MIERES, L. J., “La protección constitucional de los derechos a la intimidad y a la propia imagen en las relaciones laborales: una visión desde la jurisprudencia constitucional”, *RVAP*, núm. 99-100 (Especial “Demetrio Loperena Rota, *In memoriam*”), mayo – diciembre, 2014, pág. 2085.

⁵ STC 186/2000, de 10 de julio, FJ 4º.

⁶ STC 29/2013, de 11 de febrero, FJ 3º.

⁷ STC 241/2012, de 17 de diciembre, FJ 5º.

⁸ Como señala la jurisprudencia del Tribunal Constitucional, “*el empresario no se encuentra apoderado para llevar a cabo, bajo el pretexto de las facultades de vigilancia y control que la legislación le asigna, intromisiones ilegítimas en la intimidad de sus trabajadores en la empresa*” (STC 186/2000, de 10 de julio).

⁹ CARRILLO LÓPEZ, M., “Los ámbitos del derecho a la intimidad en la sociedad”, en *El derecho a la privacidad en un nuevo entorno tecnológico, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, pág. 41.

factor de categorización social¹⁰. Como de forma ilustrativa lo recuerda la jurisprudencia constitucional, las manifestaciones de feudalismo industrial repugnan al Estado social y democrático de derecho¹¹.

No obstante este *obiter dictum* tan significativo, una primera jurisprudencia constitucional consideraba el contrato de trabajo y las obligaciones dimanantes del mismo como elemento clave de la delimitación del derecho fundamental en la medida en que el trabajador ha dado su consentimiento¹², de manera que determinadas manifestaciones del derecho a la intimidad podían quedar desprotegidas en el ámbito laboral¹³.

En efecto, durante mucho tiempo los tribunales admitieron la utilización de medidas de control empresarial de índole tecnológico con muy pocas reservas¹⁴ bajo el entendimiento de que el centro de trabajo constituía un lugar público en donde no existía proyección del derecho de intimidad, salvo los espacios destinados al descanso y al aseo personal¹⁵. A tal efecto, la STC 142/1993, de 22 de abril, llegó a señalar que la relación de la intimidad con la dignidad personal determina que la esfera de la inviolabilidad de la persona frente a injerencias externas no comprenda, en principio, los hechos relativos a las relaciones sociales y profesionales en que se desenvuelve la prestación laboral.

De acuerdo con este razonamiento, la protección de la intimidad queda sujeta a un criterio meramente espacial regido por una teoría contractualista¹⁶ según la cual los derechos fundamentales del trabajador ceden frente al poder de dirección del empresario dado que la formalización del contrato laboral mitiga la posibilidad de su aplicación en tiempo y lugar de trabajo¹⁷ (STC 142/1993, de 22 de abril).

¹⁰ MACAVILCA ROMÁN, Z., “El derecho a la intimidad y las nuevas tecnologías. El derecho a la intimidad en el contexto de las nuevas tecnologías de comunicación e información”, en *El derecho a la intimidad. Nuevos y viejos debates*, Dykinson, Madrid, 2017, págs. 181-183.

¹¹ STC 88/1985, de 19 de julio, FJ 5.

¹² STC 6/1988, de 21 de enero, FJ 3.

¹³ SSTC 19/1985, de 13 de febrero y 170/1987, de 30 de octubre -caso del camarero con barba-. No obstante, el punto de inflexión a esta doctrina restrictiva lo supuso la STC 99/1994, de 11 de abril (caso del cortador de jamón), en la que ante las restricciones establecidas por el empresario al ejercicio de un derecho de la personalidad, como era el derecho a la propia imagen, el TC obligó a aplicar el triple test de idoneidad, necesidad y proporcionalidad a la medida restrictiva con el objeto de determinar si la misma estaba plenamente justificada y si las modulaciones ejercidas sobre el derecho fundamental del trabajador eran las estrictamente necesarias.

¹⁴ MIERES MIERES, L. J., *Intimidad personal y familiar. Prontuario de jurisprudencia constitucional*, Aranzadi, Navarra, 2002, pág. 23.

¹⁵ GUERRA RODRÍGUEZ, L., “Ejercicio del poder de control a través de cámaras de video vigilancia: análisis de la doctrina constitucional”, *Trabajo y Derecho* 29/2017 (mayo), nº 29 de 1 de mayo de 2017, pág. 2.

¹⁶ FABREGAT MONFORT, G., “El control empresarial de los trabajadores a través de las nuevas tecnologías: algunas ideas clave”, *Trabajo y Derecho*, nº 5, 2015, pág. 2.

¹⁷ En línea con lo establecido en la STC 142/1993, de 22 de abril, la STSJ de Cataluña de 25 de abril de 1994 admite la instalación de un circuito cerrado de televisión con sistema

A pesar de estos precedentes, hoy superados, la realidad indica que en el contexto de las relaciones laborales se presenta la disyuntiva entre el poder de dirección del empleador (art. 20.3 ET) y los derechos fundamentales de los trabajadores, no siendo siempre pacífica la relación entre ambos grupos de derechos, sino que suelen producirse fricciones sobre todo cuando, derivado del uso de las nuevas tecnologías, se prima la potestad de dirección del primero en detrimento de los derechos fundamentales de los segundos, ofreciendo a tal efecto la jurisprudencia, tanto constitucional como ordinaria¹⁸, numerosos ejemplos en los que se debate la proporcionalidad de la instalación de medidas de control en las empresas.

En este sentido, no hay duda alguna de que atentan contra la intimidad de los trabajadores los circuitos internos de televisión a cuyo través se accede visualmente a los vestuarios del centro de trabajo. Como tampoco, en sentido contrario, la hay respecto de la proporcionalidad de idéntica medida si el sistema de visualización queda circunscrito a las zonas de compra de productos y de pago en las cajas de un supermercado¹⁹.

No obstante, tanto en uno como en otro caso, algunos tribunales ordinarios han continuado entendiendo que en el centro de trabajo no se ejerce el derecho a la intimidad dado que el mismo se ciñe o circunscribe a un conjunto de actividades privadas que, por esencia, permanecen al margen del centro de trabajo. E incluso el Tribunal Supremo en sentencias de 26 de septiembre de 2007 y 6 de octubre de 2011 ha auxiliado un amplio ejercicio de los poderes de control del empresario al que el Tribunal Constitucional se adhirió en la STC 241/2012, de 17 de diciembre (caso del correo electrónico en la empresa), sobre la que se incidirá de forma específica más adelante, pero ya resulta necesario adelantar la contradicción que supone con el precedente sentado con anterioridad en la STC 98/2000, de 10 de abril (caso micrófonos en el casino de La Toja) en la que sostuvo que la libertad de comunicaciones viene protegida instrumentalmente a través del derecho a la intimidad²⁰.

de grabación de imagen y sonido en múltiples espacios del centro de trabajo tras considerar que entender que la medida vulnera el derecho a la intimidad “(...) supondría extender la protección de tales derechos a instalaciones que suponen la práctica totalidad de espacios públicos del hotel en el que este presta sus servicios a los clientes y, en consecuencia, donde los trabajadores desarrollan su actividad. La intimidad de estos no resulta agredida por el solo hecho de que esta sea objeto de filmación pues no se trata de divulgar su conducta, sino de obtener un conocimiento de cuál es su comportamiento laboral”. En el mismo sentido se pronuncia la STSJ de Galicia de 25 de enero de 1996.

¹⁸ Entre otras, STSJ de Madrid de 25/1/1996; STSJ de Murcia de 18/7/1995; STS de 1176/1990 (Sala IV); STSJ de Galicia, de 21/4/1995; STSJ de Cataluña, de 25/4/1994; STSJ de la Comunidad Valenciana, de 12/3/1993, etc.

¹⁹ CARRILLO LÓPEZ, M., “Los ámbitos del derecho a la intimidad...”, *op. cit.*, pág. 44.

²⁰ JIMÉNEZ PÉREZ, A., “El derecho a la intimidad en la jurisprudencia constitucional y convencional: el Tribunal Constitucional Español, el Tribunal Europeo de Derechos Humanos y la Corte Interamericana de Derechos Humanos”, en *El derecho a la intimidad. Nuevos y viejos debates*, Dykinson, Madrid, 2017, págs. 103-104.

La doctrina establecida en la referida STC 142/1993, de 22 de abril (los derechos fundamentales del trabajador ceden frente al poder de dirección del empleador), fue desautorizada posteriormente por nuestro Alto Tribunal a través de dos importantes sentencias: la 98/2000, de 10 de abril y la 186/2000, de 10 de julio, las cuales vinieron a establecer los principales criterios interpretativos en la materia, sufriendo los mismos posteriormente importantes correcciones, respecto de sus conclusiones, a través de las SSTC 29/2013, de 11 de febrero y, más recientemente, la 39/2016, de 3 de marzo. No obstante, debe advertirse que en las dos primeras el conflicto se plantea exclusivamente desde la perspectiva del derecho a la intimidad (art. 18.1 CE), quedando al margen del debate el derecho a la autodeterminación informativa que se integra en el derecho a la protección de datos personales que es, justamente, el que tuvo en cuenta la STC 29/2013, de 11 de febrero – que será objeto de análisis más adelante– y que definitivamente configura como eje de su jurisprudencia sobre la privacidad del trabajador el TEDH en su importante sentencia de 5 de septiembre de 2017 (caso *Barbulescu c. Rumanía*).

En efecto, en la STC 98/2000, de 10 de abril²¹, se rechazó el planteamiento consistente en exacerbar el poder de dirección del empresario mediante la delimitación precisa del alcance del derecho a no ser importunado en el ámbito de la actividad laboral. Esta sentencia traía su causa de la instalación por parte del Casino de La Toja de diferentes micrófonos en determinadas zonas del centro de trabajo – zona de caja y ruleta francesa –. Un trabajador que ejercía de cajero y el Comité de Empresa demandaron a la empresa por intromisión ilegítima en su derecho a la intimidad. La sentencia, estimatoria del amparo solicitado, entendió que la medida adoptada por la empresa carecía de toda proporcionalidad para alcanzar la finalidad perseguida – cual era la de garantizar la seguridad del casino – y lesionaba, por tanto, la intimidad de los trabajadores cuyas conversaciones eran grabadas de forma permanente.

En esta sentencia se afirma que el derecho a la intimidad, en cuanto derivación que es de la dignidad personal consagrada en el art. 10 CE, supone, también en el ámbito de las relaciones de trabajo, la existencia de un ámbito propio y reservado frente al conocimiento de los demás, necesario, según las pautas de nuestro sistema cultural, para el mantenimiento de una calidad mínima de vida humana, de modo que el trabajador precisa disponer de una expectativa razonable de intimidad dado que, como señala la jurisprudencia del TEDH, en su interpretación del art. 8 CEDH, sería muy restrictivo constreñir la noción de vida privada a un círculo íntimo, de modo que el derecho a la vida privada engloba también el derecho de la persona a entablar y desarrollar relaciones sociales con otras personas²² y, entre

²¹ La STC 98/2000, de 10 de abril resuelve el supuesto de la utilización en un casino (Casino de la Toja, S.A.) de micrófonos en algunas dependencias del centro de trabajo (secciones de caja y ruleta francesa) donde se grababan las conversaciones de los trabajadores. La sentencia, estimatoria del recurso de amparo, reconoce la vulneración del derecho a la intimidad personal del trabajador recurrente, y no admite que la actuación empresarial tuviera, en el caso concreto, amparo en las facultades de vigilancia y control reconocidas al empresario por la legislación laboral (art. 20.3 ET).

²² STEDH de 16 de diciembre de 1992, caso *Niemietz c. Alemania*.

esas relaciones, deben incluirse – obviamente – las relaciones laborales, por lo que la captación de imágenes y sonidos no puede ser en ningún caso indiscriminada²³.

A este efecto, cabe señalar que el art. 7 de la LO 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad personal y Familiar y a la Propia Imagen, establece que tendrán la consideración de intromisiones ilegítimas : “1) *El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas*; 2) *La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción*”.

La formulación genérica de esta Ley requiere de la necesaria matización a la luz de la jurisprudencia constitucional, siendo la principal cuestión que cabe plantear la de si el empleador se encuentra legitimado para poder instalar aparatos de escucha en la empresa y si tal decisión conlleva inexorablemente una lesión del derecho a la intimidad del trabajador. Y la primera reflexión que hemos de efectuar al respecto es la de que el derecho a la intimidad de la persona no queda circunscrito espacialmente a su domicilio personal, sino que la empresa es también un escenario físico-espacial de carácter público en el que la persona comparte su actividad con otras, existiendo en la misma zonas en las que el derecho a no ser perturbado le sigue acompañando²⁴.

Como ha puesto de relieve el TC, la expectativa razonable de privacidad se relaciona con el derecho de la persona a mantener una “barrera de reserva”²⁵ en sus diversos ámbitos relacionales, incluido – obviamente – el laboral. Así, por ejemplo, forman parte de este ámbito privado el comedor, los vestuarios o las zonas de esparcimiento de la empresa, sin obviarse otros espacios en los que el derecho fundamental a la intimidad sigue vigente aunque se esté desempeñando una actividad laboral, siendo esta precisamente la razón por la que el Tribunal Constitucional rechaza la premisa, de la que parten algunas sentencias de la jurisdicción ordinaria, según la cual el centro de trabajo no es un espacio en el que se ejerza aquel derecho.

De este modo, para la determinación de la procedencia de la instalación de sistemas de videovigilancia resulta necesario atender no solo a las características del centro de trabajo, sino también a otros elementos causales, tales como el hecho de si la instalación del sistema ha sido o no indiscriminada²⁶ o si ha sido hecha de forma subrepticia²⁷ o cuál sea la finalidad realmente perseguida, si concurren razones

²³ CARRILLO LÓPEZ, M., “Los ámbitos del derecho a la intimidad...”, *op. cit.*, pág. 46.

²⁴ CARRILLO LÓPEZ, M., “Los ámbitos del derecho a la intimidad...”, *op. cit.*, pág. 46.

²⁵ SSTC 99/1994, de 11 de abril, FJ 4º; 156/2001, de 2 de julio, FJ 3º; 72/2007, de 16 de abril, FJ 5º y 77/2009, de 23 de marzo, FJ 2º.

²⁶ Vid. STEDH de 9 de enero de 2018 (caso López Ribalda *et alii* c. España).

²⁷ En este sentido cabe citar la STS de 13 de mayo de 2014 (Sala IV, Sección 1ª), que considera vulnerado el derecho a la intimidad de una trabajadora derivado de la utilización de cámaras de videovigilancia instaladas, como sistema disuasorio de hurtos por parte clientes, por causa de la falta de información sobre la posibilidad de supervisión laboral de las capturas de imágenes de los trabajadores y sin que por parte del empresario estuviesen

objetivas de seguridad, etc. En suma, habrá que tener en consideración si la instalación de estos sistemas de videovigilancia y control responde a verdaderos criterios de proporcionalidad, dado que, si bien es cierto que son medidas que se insertan en el ámbito del poder directivo empresarial, no pueden, sin embargo, conducir a resultados inconstitucionales²⁸.

En el caso de la instalación de micrófonos en la zona de caja y ruleta francesa resulta evidente que la misma permite la captación y grabación de conversaciones que se producen en dichos lugares entre los trabajadores y clientes del casino y entre los propios trabajadores. Al margen de que razones de seguridad puedan justificar esta medida – la cual fue adoptada como complemento de otras ya existentes –, resulta obvio que, a través de la misma, es plenamente factible la captación y grabación de cualesquiera conversaciones mantenidas por los trabajadores a lo largo de su jornada laboral que poco o nada tengan que ver con su desempeño profesional y sí, sin embargo, con su intimidad, la cual es y debe de ser inaccesible a terceros.

Supuesto diferente es el que nos brinda la decisión de instalar cámaras para un circuito cerrado de televisión en las cajas registradoras del economato de un centro de trabajo ante la sospecha de irregularidades contables en la sección de textil y calzado (STC186/2000, de 10 de julio, caso de las cámaras en el economato de ENSIDESA). Esta sentencia resuelve el caso de un despido disciplinario en el que se imputa al trabajador la sustracción de dinero de la caja de dicho economato, habiendo utilizado la empresa para acreditar la conducta las grabaciones del sistema de videovigilancia que instaló para comprobar sus sospechas. Los Tribunales declararon la procedencia del despido no apreciando vulneración alguna del derecho a la intimidad del trabajador derivada de la instalación de las cámaras de vigilancia. El TC desestima el recurso de amparo considerando que, en el caso de autos, se respetó por la empresa el derecho a la intimidad del trabajador y que las pruebas videográficas eran válidas, al tiempo que reitera la doctrina de la STC 98/2000, de 10 de julio, y fija como criterios a tener en cuenta los siguientes:

i) El derecho fundamental a la intimidad despliega toda su eficacia también en el seno de las relaciones jurídico laborales, si bien no se trata de un derecho ilimitado o absoluto, sino que el mismo puede ceder ante intereses constitucionales tal como sucede en los casos en que la modulación que aquel hubiere de experimentar se revelare como necesaria para la consecución del fin legítimo previsto, fuere proporcionada para alcanzarlo, así como respetuosa con el contenido esencial del derecho²⁹.

ii) El poder de dirección del empleador, contemplado en el art. 20.3 ET, atribuye a este la facultad de adoptar medidas de control y vigilancia en orden a la verificación del cumplimiento por parte del trabajador de sus obligaciones laborales, respetando, eso sí, en todo momento la dignidad del trabajador (arts. 4.2.c) y 20.3 ET).

previstos dispositivos anunciando su instalación y captación de imágenes, así como la notificación de la creación de ficheros a la AEPD.

²⁸ CARRILLO LÓPEZ, M., “Los ámbitos del derecho a la intimidad...”, *op. cit.*, pág. 47.

²⁹ SSTC 57/1994, de 28 de febrero, FJ 5º y 143/1994, de 9 de mayo, FJ 4º.

iii) El empresario carece de legitimidad para llevar a cabo intromisiones ilegítimas en la intimidad de sus trabajadores en el centro de trabajo bajo el pretexto de las citadas facultades de vigilancia y control previstas en el art. 20.3 ET.

2.1 Control del Ordenador y Derechos Fundamentales del Trabajador.

El silencio legislativo imperante hasta diciembre de 2018³⁰ acerca de la cuestión del control del ordenador asignado al trabajador para el desarrollo de su prestación laboral ha dado lugar a un intenso debate hasta finales de la década pasada. Ante el silencio del legislador resultaban posibles diferentes aproximaciones doctrinales. De un lado, era posible pensar que el ordenador era estrictamente una herramienta de trabajo, de modo que había que reconocer una extensa facultad de control a favor del empresario en cuanto titular de los medios de producción. De otro lado, cabía pensar también que, aun siendo titularidad de la empresa, el ordenador es una herramienta peculiar en la medida en que puede contener datos privados del trabajador, de forma que no resulta posible reconocer tan extensas posibilidades de vigilancia de su contenido por cuanto ello puede suponer un sacrificio del derecho a la intimidad de este, por lo que el control ha de quedar supeditado al cumplimiento de los requisitos materiales y formales establecidos en el art. 18 ET en orden al registro de los efectos personales del trabajador³¹.

Desembocada la cuestión ante el Tribunal Supremo, este procedió a unificar doctrina mediante la sentencia de 26 septiembre 2007. El TS se situó en un punto intermedio entre ambas tendencias reconociendo, en línea con la primera, que el ordenador se incluye entre los medios, propiedad de la empresa, que esta pone a disposición del trabajador para que los utilice en el cumplimiento de su prestación de trabajo, de modo que ese uso cae bajo la órbita del poder de vigilancia y control del empresario, no aplicándose, por tanto, la regla especial del art. 18 ET, sino la general del art. 20.3 ET.

Ahora bien, dadas las dificultades de índole práctico en orden al establecimiento de una prohibición absoluta del uso personal del ordenador y de una cierta tolerancia acerca de un uso moderado de los medios de la empresa, aceptó, alineándose de este modo con la segunda, la existencia de una “expectativa general de confidencialidad” de los eventuales usos privados. La forma de equilibrar ambas ideas se encuentra en el tratamiento de esta expectativa, la cual no puede ser ignorada, pero tampoco erigirse en un impedimento permanente para el control del empresario. De hecho, este resulta admisible en función de las instrucciones establecidas por este para el uso del ordenador y de acuerdo con los controles que se hayan previstos para verificar esa utilización.

³⁰ Esta cuestión ha sido regulada por el art. 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

³¹ GOERLICH PESET, J. M^a., “Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas”, en *El derecho a la privacidad en un nuevo entorno tecnológico, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, pág. 144.

La evolución interpretativa posterior, tanto en la doctrina del TS como en la jurisprudencia constitucional, ha clarificado el alcance de esta doctrina. Y, al hacerlo, ha ampliado las facultades empresariales de control respecto de las que parecían deducirse literalmente del primer pronunciamiento, habiendo seguido esta ampliación diferentes líneas. En primer lugar, en relación con la contribución del trabajador a la generación de la expectativa general de confidencialidad, la STS de 26 de septiembre 2007 no parece condicionar su nacimiento a requerimientos especiales en la conducta del trabajador al señalar que no constituye obstáculo alguno para la protección de la intimidad el hecho de que el ordenador no tuviera clave de acceso ni que el mismo estuviera situado en un despacho sin llaves.

Sin embargo, la posterior STC 241/2012, de 17 de diciembre, valora para excluir la lesión del derecho fundamental, entre otras circunstancias, que las comunicaciones privadas se habían producido al haberse introducido el programa en un soporte de uso común para todos los empleados de la empresa sin haberse observado la más mínima cautela al efecto.

Por otro lado, la STS de 26 de septiembre 2007 parece pensar en la existencia de un protocolo en cada empresa sobre el uso del ordenador afirmando, al respecto, que lo que ha de hacer el empresario, de acuerdo con las exigencias de la buena fe, es establecer con carácter previo las reglas de uso del mismo – estableciendo prohibiciones absolutas o parciales – e informar a los trabajadores tanto de que se va a proceder a controlar el uso del ordenador como de los medios que se van a utilizar a tal fin. Asimismo, la jurisprudencia social del TS parece pensar en un control limitado mediante monitorizaciones de carácter general, excluyéndose la vigilancia singularizada³².

Sin embargo, la doctrina posterior ha permitido la prohibición absoluta del uso privado del ordenador, posibilitando un control empresarial completo de su utilización por parte del trabajador, habiendo sido esta la postura sostenida, primero por el TS en sentencia de 6 octubre 2011 y, más recientemente, por el TC en sentencia 170/2013, de 7 octubre³³, si bien esta posición ha quedado en entredicho a raíz de la STEDH de 5 de septiembre de 2017 en el caso *Barbulescu c. Rumanía*, que proscribe la reducción a cero del ejercicio de los derechos fundamentales del trabajador en el seno de la empresa³⁴.

En este punto hay que hacer notar que esta evolución ha supuesto una notable ampliación del ámbito al que se aplica la expectativa general de confidencialidad. Si bien los primeros pronunciamientos se referían al uso por el trabajador del ordenador y de Internet (aplicaciones utilizadas, eventuales archivos privados existentes en él y, sobre todo, secuencia de navegación en la Red tales como sitios visitados, tiempos de visita, etc.), posteriormente la jurisprudencia ha extendido esta

³² STS de 8 marzo 2011, FJ 5º.

³³ GOERLICH PESET, J. Mª., “Protección de la privacidad de los trabajadores...”, *op. cit.*, pág. 145.

³⁴ Dice expresamente la STEDH de 5 de septiembre de 2017 (caso *Barbulescu c. Rumanía*) que “*sea como fuere, las instrucciones de un empleador no pueden reducir la vida social privada del trabajador a cero. El respeto de la vida privada y de la confidencialidad de la correspondencia siguen existiendo aun cuando estas pudieran estar restringidas en la medida de lo necesario*”.

categoría a supuestos en los que pudiera ser aplicable una protección constitucional más fuerte como es la derivada del secreto de las comunicaciones. Si históricamente el TS había aceptado la posible interceptación de las comunicaciones telefónicas en los casos en los que la prestación consistía precisamente en hacer o atender llamadas³⁵, en fecha más reciente se ha extendido la posibilidad de control empresarial a los programas de mensajería instantánea ubicados en ordenadores de la empresa³⁶ y a las direcciones corporativas de correo electrónico³⁷.

Los conflictos derivados del control, por parte del empresario, del uso de los ordenadores y el derecho a la intimidad de los trabajadores devienen del hecho de que aquellos pueden ser usados tanto para cuestiones de índole estrictamente laboral como para temas personales, siendo este el punto del cual parte la STS (Sala IV) de 26 de septiembre de 2007 – fundamental en el tema que se analiza – que sostiene que dichos conflictos surgen dada la existencia de un uso personal – y no exclusivamente laboral – del medio facilitado por la empresa³⁸. En relación con el correo electrónico cabe señalar que el derecho al secreto de las comunicaciones impide que el empresario pueda interceptar las comunicaciones que pudieran mantener los trabajadores entre sí, o con personas ajenas a la compañía, vía correo electrónico o chat³⁹.

No obstante, recientemente, el art. 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, reconoce y regula el derecho a la intimidad de los trabajadores en la utilización de dispositivos digitales puestos a su disposición por el empleador autorizando al empresario a acceder al contenido de los dispositivos a los solos efectos de controlar el cumplimiento de las obligaciones laborales y de garantizar la integridad de dichos dispositivos, debiendo las empresas establecer criterios de utilización de los mismos

³⁵ STS de 5 diciembre 2003, FJ 3º.

³⁶ STC 241/2012, de 17 de diciembre, FJ 4º.

³⁷ STS de 6 octubre 2011, FJ 2º y STC 170/2013, de 7 octubre, FJ 3º.

³⁸ Para VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa*, Universidad Rey Juan Carlos, Madrid, 2011, pág. 81, los archivos derivados del uso laboral del ordenador de la empresa por parte del trabajador no forman parte del ámbito privativo de este, en tanto que aquellos otros vinculados al uso personal por parte de aquel sí caerían dentro de la categoría de privados y, por tanto, protegidos por el derecho a la intimidad.

Estamos en desacuerdo con esa apreciación dado que cualquier archivo es susceptible de contener información perteneciente al ámbito privativo del trabajador, de modo que la diferenciación vendría dada por el contenido de la información incluida en el archivo digital de que se trate.

³⁹ Para VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales...*, *op. cit.*, págs. 82-83, si se trata de mensajes almacenados, ya lo fueran por el remitente como por el destinatario, si ya hubieran sido abiertos y leídos no operaría el derecho al secreto de las comunicaciones, de modo que en relación con los mismos cabría plantear si el acceso a su contenido afecta al derecho a la intimidad y la repuesta que cabe dar a este interrogante es que dependerá siempre del contenido de la comunicación, de modo que solo los mensajes de correo electrónico cuyo contenido fuere de carácter personal y reservado podrían plantear problemas relativos al derecho a la intimidad.

respetando los estándares mínimos de protección de la intimidad y con la participación de los representantes de los trabajadores.

Por su parte, el acceso a los dispositivos respecto de los que se hubiere admitido una utilización con fines privados requerirá de una precisa y concreta especificación de los usos autorizados y prohibidos, así como del establecimiento de garantías para la preservación de la intimidad, tales como la especificación de los períodos o momentos temporales en los que los dispositivos podrán ser usados para fines privados, debiendo informarse a los trabajadores de esos criterios de utilización.

Por lo que respecta a la navegación por Internet, la misma supone la entrada de datos en el ordenador los cuales quedan incorporados en este pudiendo ser los mismos rastreados de forma que se puede conocer, bien sea en tiempo real o con posterioridad, la actividad desarrollada por el usuario del equipo en la Red.

Sobre el particular, el Documento aprobado el 29 de mayo de 2002 por el Grupo de trabajo del artículo 29 de la Directiva 95/46/CE contiene una serie de recomendaciones acerca del control del acceso a Internet en el seno de las organizaciones empresariales, desaconsejando prohibiciones absolutas de la utilización de la Red con fines personales por parte de los trabajadores, al tiempo que insiste en la necesidad de que el empresario informe a los trabajadores sobre las condiciones de uso de Internet y de los posibles sistemas de control que se pudieran establecer para controlar dicho uso.

Por su parte, el TEDH ha entendido que la utilización personal de Internet atañe a los conceptos de “vida privada” y “correspondencia” del artículo 8.1 del CEDH, de modo que la monitorización y/o control de la actividad del trabajador en la Red puede suponer una injerencia en los derechos contemplados en dicho precepto⁴⁰ toda vez que la información así obtenida puede albergar datos sensibles relativos a la intimidad de la persona por contener información referida a aspectos de su vida privada tales como su ideología, sus creencias religiosas, su orientación sexual, sus aficiones, etc.

En base a ello, la STS (Sala IV) de 26 de septiembre de 2007 encuadra dentro del concepto de intimidad las huellas derivadas de la navegación en Internet al señalar que esos archivos caen dentro del ámbito de protección de la intimidad, de modo que el acceso a los archivos temporales de Internet y, de modo genérico, a cualesquiera huellas derivadas de la navegación por la Red que queden incorporadas al equipo puede afectar a la intimidad del usuario y generar la ilicitud de las pruebas así obtenidas⁴¹.

En definitiva, lo determinante para evaluar si el acceso a un fichero informático puede suponer una afección del derecho a la intimidad es que el contenido del mismo pueda contener o no información perteneciente al “ámbito propio y reservado” del trabajador, a cuyo efecto existe una abundante jurisprudencia delimitadora de las materias que pueden afectar a dicho ámbito. Sin ánimo de exhaustividad, conforme a la jurisprudencia del TC, se puede considerar

⁴⁰ Vid. STEDH de 3 de abril de 2007 (caso Copland c. Reino Unido).

⁴¹ VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales...*, op. cit., pág. 83.

que afectan al derecho a la intimidad las intromisiones referidas, entre otras, a las siguientes materias⁴²:

- a) La intimidad corporal, la cual protege frente a intromisiones que pudieran llegar a constituir violación del recato o pudor de la persona⁴³.
- b) Las informaciones referentes a la salud, tanto física como psíquica, de las personas⁴⁴.
- c) Las informaciones relativas al consumo de drogas y/o alcohol⁴⁵.
- d) Los datos afectantes a la situación económica de una persona⁴⁶.
- e) Las informaciones sobre detalles concretos de la vida en el seno del hogar familiar⁴⁷, etc.

Como se ha dicho, no se trata de un elenco elaborado con ánimo de exhaustividad, sino de una simple exposición de hipótesis extraídas de casos decididos por el TC, lo cual permite la posibilidad de que otras tantas materias puedan quedar engullidas en el ámbito privativo de la persona y susceptible, pues, de afectar al derecho a la intimidad de esta dado que, como acertadamente señala Rodríguez Piñero y Bravo-Ferrer⁴⁸, una de las cuestiones problemáticas que plantea el derecho fundamental a la intimidad es su compleja determinación sustantiva habida cuenta de que el mismo abarca tanto espacios de la vida personal y familiar como cuestiones relativas a la sexualidad, a la dignidad, a la imagen, etc., de modo que la investigación del contenido almacenado en el ordenador del trabajador supondrá una vulneración de su derecho a la intimidad siempre que aquella se refiera a materias comprendidas en el ámbito “propio y reservado” de aquel, por lo que la aportación a un proceso de dichos materiales probatorios plantearía serios problemas de ilicitud de los mismos.

2.1.1 Existencia de Expectativa Razonable de Privacidad

El TEDH acota los supuestos en los que el acceso a datos privados puede constituir una intrusión en el derecho al respeto de la vida privada y familiar en

⁴² VEGAS TORRES, J., *Idem*, págs. 84-85.

⁴³ SSTC 196/2004, de 15 de noviembre, FJ 4º; 218/2002, de 25 de noviembre, FJ 5º y 57/1994, de 28 de febrero, FJ 4º, entre otras.

⁴⁴ SSTC 159/2009, de 29 de junio, FJ 2º y 70/2009, de 23 de marzo, FJ 3º.

⁴⁵ SSTC 206/2007, de 24 de septiembre, FJ 4º; 196/2004, de 15 de noviembre, FJ 5º y 207/1996, de 16 de diciembre, FJ 4º.

⁴⁶ SSTC 233/2005, de 26 de septiembre, FJ 4º y 233/1999, de 16 de diciembre, FJ 3º.

⁴⁷ STC 115/2000, de 10 de mayo, FJ 5º.

⁴⁸ RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M., “Derecho a la intimidad del trabajador y contrato de trabajo”, en *Diario La Ley*, núm. 6033, de 4 de junio de 2004.

función de que exista o no, en el caso concreto, de una “expectativa razonable de privacidad”⁴⁹.

Así, en su sentencia de 5 de junio de 1997 (caso Halford c. Reino Unido) el tribunal rechaza la argumentación del Gobierno británico relativa al hecho de que el empresario tuviera derecho a controlar, sin necesidad de advertencia previa, las llamadas telefónicas realizadas por sus trabajadores con el teléfono de la empresa, sosteniendo que, por el contrario, conforme a su reiterada jurisprudencia, resulta evidente que las llamadas telefónicas realizadas desde la oficina – lo mismo que las efectuadas desde el domicilio particular – caen dentro del concepto de “vida privada” y “correspondencia” del art. 8.1 del CEDH, sosteniendo el tribunal que no hay constancia alguna acerca de que se hubiere advertido a la funcionaria demandante sobre el hecho de que las llamadas realizadas desde los terminales de su despacho oficial pudieran ser objeto de intervención, siendo así que el tribunal entiende que la funcionaria gozaba de una “expectativa razonable de privacidad” respecto de las mismas, la cual se veía incluso reforzada por factores coadyuvantes tales como su elevado rango, que determinaba que pudiera disfrutar de un despacho propio con dos teléfonos, uno de los cuales era para uso privado y, por lo demás, sus superiores jerárquicos habían autorizado de modo expreso que utilizara los teléfonos de su despacho para el mantenimiento de conversaciones relacionadas con la reclamación por discriminación efectuada por ella y con motivo de la cual se produjeron las interceptaciones⁵⁰.

Por su parte, en el caso Copland c. Reino Unido (sentencia de 3 de abril de 2007) se resuelve un caso en el que las llamadas telefónicas, así como el correo electrónico y la navegación por la Red de una empleada de un *College* público habían sido controladas por un superior jerárquico, aplicando de nuevo el TEDH el denominado test de la “expectativa razonable de privacidad” en orden a la determinación de si los hechos enjuiciados quedaban o no englobados en el ámbito de aplicación del art. 8 CEDH, a cuyo efecto el tribunal sostiene que su doctrina jurisprudencial referida a las llamadas telefónicas efectuadas desde el lugar de trabajo resulta también de aplicación tanto al uso del correo electrónico de la empresa como a la información derivada del control del uso personal de la Red por quedar ambos comprendidos en la noción de “vida privada” y “correspondencia” del art. 8.1 del CEDH. Y, dicho esto, el tribunal constata que, además, no se advirtió de modo expreso a la demandante acerca de que sus llamadas podían ser objeto de monitorización, de modo que la trabajadora gozó, en todo momento, de una expectativa razonable de privacidad respecto de las llamadas efectuadas desde los terminales del lugar de trabajo, la cual es extensible también al uso del correo electrónico y a la navegación por Internet⁵¹.

⁴⁹ VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales...*, op. cit., pág. 97.

⁵⁰ VEGAS TORRES, J., *Idem.*, *Ibidem*.

⁵¹ VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales...*, op. cit., pág. 97.

Asimismo, en el caso *Peev c. Bulgaria* (sentencia de 26 de julio de 2007⁵² se vuelve a aplicar el test de la “expectativa razonable de privacidad” para alcanzar la conclusión de que el registro efectuado había defraudado dicha expectativa de la cual gozaba el demandado, suponiendo, por tanto, aquella una injerencia en los derechos del art. 8.1 del CEDH, argumentando a tal efecto el TEDH que en todo caso debe entenderse existente un acuerdo implícito en las relaciones empresario-trabajador que permite a estos últimos la posibilidad de tener objetos personales en los cajones de las mesas de trabajo y en los archivadores del despacho, asentándose en este acuerdo la expectativa razonable de privacidad que el tribunal reconoce al demandante, la cual determina que se considere que el registro realizado afecta a los derechos del art. 8.1 Convenio, si bien el tribunal admite, asimismo, la posibilidad de que el empresario pueda establecer políticas que prohíban o limiten la posibilidad de tener objetos personales por parte de los empleados en sus mesas y archivadores, lo cual podría excluir la expectativa razonable de privacidad de aquellos en caso de incumplimiento de tales políticas⁵³.

En línea con lo establecido por la jurisprudencia del TEDH, el Tribunal Supremo en sentencia de 26 de septiembre de 2007 afronta el análisis de un caso sometido a su consideración relacionándolo con la existencia o no de una “expectativa de privacidad” del trabajador con respecto a los contenidos guardados en el ordenador de la empresa, sosteniendo que, en la medida en que se pudiera considerar existente dicha expectativa de privacidad, el acceso por parte del empresario a datos privados del trabajador podría suponer una intromisión en su derecho fundamental a la intimidad, mientras que si, en función de las circunstancias del caso, no se pudiera afirmar que los trabajadores gozaran de una expectativa razonable de privacidad, el derecho a la intimidad de los mismos no podría considerarse afectado⁵⁴.

En este sentido, tanto la jurisprudencia del TEDH como del TC y del TS parten de la base de la existencia de una expectativa de privacidad relacionada con los contenidos personales que el empleado tuviere en el ordenador de la empresa. A este respecto, cabe referenciar las sentencias del TEDH relativas a los casos *Halford* y *Copland c. Reino Unido* que asumen que, a falta de advertencia expresa acerca del hecho de que tanto las conversaciones telefónicas como el uso personal del correo electrónico y la navegación por Internet realizados con los medios de la empresa pueden ser controlados, hay que entender latente una expectativa razonable de privacidad respecto del contenidos de tales comunicaciones.

En este orden de cosas, hay que recordar la sentencia del TEDH recaída en el caso *Peev c. Bulgaria*, la cual parte del hecho de que existe un acuerdo implícito, habitual en las relaciones de trabajo, que autoriza a los empleados a almacenar

⁵² El caso *Peev c. Bulgaria* analiza el caso de un empleado público cuyo despacho había sido registrado por orden de su superior en el marco de unas actuaciones de carácter disciplinario hallándose en dicho registro diferentes efectos de carácter personal del demandante tanto en los cajones del escritorio como en los archivadores.

⁵³ VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales...*, op. cit., págs. 98-99.

⁵⁴ VEGAS TORRES, J., *Idem.*, pág. 96.

objetos de índole personal en las mesas y archivadores del puesto de trabajo del que deriva una expectativa de privacidad de aquellos respecto de estos⁵⁵.

Por su parte, el Tribunal Constitucional es determinante en rechazar los planteamientos tendentes a la exclusión de la existencia de cualquier expectativa razonable de privacidad en el ámbito de la empresa, siendo muy expresiva a este respecto la STC 98/2000, de 10 de abril, que rechaza de forma expresa el entendimiento de que el centro de trabajo no constituye un espacio en el que se pueda ejercer el derecho a la intimidad por parte de los empleados.

De igual modo, la referida STS (Sala 4ª) de 26 de septiembre de 2007 analiza de forma expresa el tema de la existencia de una expectativa de privacidad en relación con los datos de índole personal de los trabajadores guardados en el ordenador de la empresa, considerando que el derecho a la intimidad puede verse en entredicho por el acceso por parte del empresario a los siguientes tipos de archivos: i) correo electrónico; ii) archivos personales del trabajador almacenados en el ordenador, y iii) archivos temporales de Internet, así como las huellas de la navegación en la Red, partiendo dicha sentencia de la existencia de un hábito social de tolerancia respecto de determinados usos personales moderados de los medios informáticos facilitados por la empresa y que dicha tolerancia crea también una expectativa de confidencialidad en tales usos⁵⁶.

3. No obstante, al fijarse el fundamento de la protección constitucional y europea en la existencia de una expectativa de privacidad, se admite la posibilidad de que dicha protección pueda quedar desactivada cuando el acceso por parte del empleador a los datos de índole personal que contenga el ordenador del empleado no defraudare ninguna expectativa razonable de confidencialidad⁵⁷.

En este sentido, la STS de 26 de septiembre de 2007 alude a la posibilidad de que el empresario pueda limitar o modular la expectativa de confidencialidad a través del establecimiento de reglas concretas de uso de los dispositivos informáticos de la empresa que determinen si está permitido o no –y si no lo está, en qué medida no lo está – el uso privado y las medidas de control que aplicará al efecto, de modo que la existencia y el conocimiento de unas y otras por parte de los trabajadores podrían modular la expectativa de confidencialidad acerca del uso privado de las herramientas informáticas de la empresa, teniendo siempre como límite dichas reglas de uso la dignidad del trabajador, en cuanto fundamento de todos los derechos fundamentales de la persona, así como las prescripciones derivadas de la STEDH de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía) que, como se ha dicho, proscribía la reducción a cero del ejercicio de los derechos fundamentales en el seno del contrato de trabajo al establecer expresamente que las instrucciones de un empresario no pueden reducir de modo absoluto la vida social privada del

⁵⁵ VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales...*, *op. cit.*, pág. 101.

⁵⁶ VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales...*, *op. cit.*, pág. 101.

⁵⁷ En este sentido, cabe señalar la alusión en las SSTEDH en los casos Halford y Copland c. Reino Unido a la inexistencia de una advertencia previa de carácter expreso al trabajador acerca de que sus comunicaciones y el uso personal de Internet podían ser controlados.

trabajador, sino que el respeto de la vida privada y de la confidencialidad de la correspondencia siguen existiendo aun cuando estas pudieran estar restringidas en la medida de lo necesario.

En resumen, con base en la doctrina formulada por la STS de 26 de septiembre de 2007 podemos afirmar que:

i) Lo verdaderamente importante de la doctrina que en ella se unifica no es la valoración conductual del trabajador a efectos disciplinarios, sino los límites del poder de control del empresario en relación al uso del ordenador facilitado por la compañía.

Concretamente, son dos los aspectos fundamentales sobre los que se pronuncia la sentencia unificadora de doctrina, a saber: (i) el empleador puede controlar el uso dado por el empleado al ordenador de la empresa, el cual no se regula por el art. 18 ET, sino por el art. 20.3 ET; y (ii) para que ese control sea lícito, el empresario habrá de concretar con carácter previo las reglas de uso del ordenador e informar a los trabajadores acerca de la existencia de controles, así como de las medidas a aplicar en caso de incumplimiento de tales reglas⁵⁸.

ii) El acceso por parte del empleador a archivos personales contenidos en el ordenador del trabajador puede suponer una injerencia en el derecho a la intimidad de este si, atendidas las circunstancias concretas del caso, el trabajador contara con una expectativa razonable de confidencialidad referida a esos archivos.

A tal efecto, el TS sostiene que la existencia de un hábito social generalizado de tolerancia respecto de ciertos usos personales de carácter moderado de los medios informáticos de la empresa genera para el trabajador una expectativa de confidencialidad en tales usos que no puede ser desconocida a la hora de llevar a cabo el control empresarial, aunque tampoco puede convertirse en un impedimento de tipo permanente para el control del empresario porque, aunque el trabajador tiene derecho a que se respete su intimidad, este no puede pretender imponer ese respeto cuando utiliza un instrumento suministrado por la empresa en contra de las indicaciones dadas por esta para su uso⁵⁹.

iii) De lo anterior extrae el TS una nueva conclusión señalando que lo que ha de hacer el empresario, de conformidad con las exigencias del principio de buena fe, es establecer con carácter previo las reglas de uso de los medios informáticos y de comunicación de la empresa e informar a los trabajadores de la posibilidad de que existan controles y de los medios que se aplicarán para comprobar la corrección de la utilización de los mismos. De esta forma, si los medios informáticos se utilizaren para usos privados, mediando prohibición concreta al efecto y conociendo el trabajador los controles que se aplicarán, no podrá concluirse que, al realizarse el control, se ha vulnerado una expectativa de intimidad.

iv) Asimismo, extiende el TS la garantía de la intimidad a los archivos temporales, que son copias que se almacenan automáticamente en el disco duro de las páginas web visitadas. En realidad se trata de huellas de la navegación por la Red

⁵⁸ PONCE RODRÍGUEZ, S., “El poder de control empresarial sobre los medios informáticos puestos a disposición del trabajador. Sentencia del Tribunal Supremo de 26 de septiembre de 2007”, *Revista Actualidad Jurídica Uría Menéndez*, núm. 19, enero-abril 2008, pág. 68.

⁵⁹ PONCE RODRÍGUEZ, S., *Idem.*, *ibídem*.

y no de informaciones de índole personal, si bien el TS entiende que tales archivos también entran dentro de la protección de la intimidad⁶⁰. Así lo establece, por lo demás, la sentencia de 3 de abril de 2007 del TEDH (caso Copland c. Reino Unido) cuando señala que está incluida en la protección del art. 8 del Convenio la información obtenida del seguimiento del uso personal de Internet dado que puede albergar datos sensibles que atenten contra la intimidad en la medida en que puede incorporar información reveladora de determinados aspectos de la vida privada tales como la ideología, las aficiones personales, la orientación sexual, etc.

v) Constituye una carga para el empresario el establecimiento de reglas de uso y control que sean conocidas expresamente por los trabajadores en el sentido de que, si no lo hiciera, no podrá obtener pruebas lícitas en orden a la defensa ante los tribunales de justicia de las medidas disciplinarias que pudiera adoptar.

Señalar que gran parte de esta doctrina ha sido acogida por el art. 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

vi) Por último, aunque la sentencia de casación que comentamos otorgó en su momento una cierta seguridad jurídica respecto de algunos de los puntos controvertidos en torno al control del empleador, lo cierto es que también dejó sin respuesta determinados aspectos sobre la materia, siendo la principal cuestión no aclarada la relativa al derecho al secreto de las comunicaciones.

2.1.2 El acceso a contenidos privados mediante consentimiento del trabajador afectado

En caso de que el trabajador prestare su consentimiento para que el empleador accediere a contenidos referidos a su actividad informática que tuvieren un carácter privado, el derecho a la intimidad de aquel no resultaría afectado y la prueba así obtenida no podría ser tachada de ilícita.

Según reiterada jurisprudencia del TC, el derecho a la intimidad otorga una facultad de exclusión que impone a terceros un deber de abstenerse de realizar intromisiones salvo que las mismas estuvieren fundadas en una previsión legal con base constitucional y fueren proporcionadas o bien existiere un consentimiento eficaz que las autorizara, habida cuenta de que corresponde a cada persona el acotamiento del ámbito de su intimidad personal y familiar que preserva del conocimiento ajeno⁶¹, de modo que el derecho a la intimidad resultará vulnerado cuando la injerencia en el ámbito reservado de la persona no fuere acorde con la ley, no fuese eficazmente consentida o, siendo la misma autorizada, subvirtiera el alcance para el que se otorgó el consentimiento⁶².

⁶⁰ PONCE RODRÍGUEZ, S., “El poder de control empresarial sobre los medios informáticos...*op. cit.*, pág. 69.

⁶¹ SSTC 196/2004, de 15 de noviembre, FJ 5º; 83/2002, de 22 de abril, FJ 3º; 44/1999, de 5 de abril, FJ 3º; 207/1996, de 16 de diciembre, FJ 4º; 292/2000, de 30 de noviembre, FJ 5º y 70/2002, de 3 de abril, FJ 4º.

⁶² SSTC 70/2009, de 23 de marzo, FJ 4º y 196/2004, de 15 de noviembre, FJ 5º.

Por tanto, para que el consentimiento del trabajador a cuya información privada se accediere excluya una hipotética lesión del derecho a la intimidad, el mismo habrá de reunir la cualidad de la eficacia⁶³, a lo que hay que unir el hecho de que la información personal así obtenida habrá de ser utilizada para la finalidad para la que se otorgó el consentimiento y no a otra diferente⁶⁴.

Respecto de la eficacia del consentimiento, la jurisprudencia del TC viene exigiendo que la persona ha de estar previamente informada del alcance y consecuencias de su consentimiento⁶⁵, afirmando la STC 196/2004, de 15 de noviembre, que el sujeto afectado habrá de contar con una información adecuada para que el consentimiento sea un acto informado y pleno⁶⁶, a lo que hay que añadir el hecho de que el consentimiento se presta para fines concretos, los cuales habrán de ser explicitados en la información previa ofrecida al afectado⁶⁷, de modo que, teniendo presente la finalidad para la que se otorgó el mismo, el acceso a datos privados que nada tengan que ver con dicha finalidad no quedará cubierto por el consentimiento prestado por la persona vulnerándose, pues, el derecho a la intimidad.

De cuanto antecede se infiere que para que el acceso por parte del empresario a datos privados del trabajador que estuvieren contenidos en el ordenador de la empresa se considere cubierto por el consentimiento de este será necesario el concurso de los siguientes requisitos, a saber: i) información previa de carácter expreso al trabajador acerca del alcance y finalidad de la investigación empresarial a realizar; ii) prestación eficaz del consentimiento por parte del trabajador al carácter de la investigación, su alcance y finalidad; y iii) la investigación no podrá exceder del alcance referido, así como tampoco sus resultados podrán ser usados para una finalidad diferente de aquella para la que el trabajador prestó su consentimiento⁶⁸.

Desde esta óptica, en caso de que el trabajador requiriese la intervención de técnicos para reparar deficiencias de funcionamiento del equipo informático del

⁶³ En relación a los mensajes automáticos en pantalla, se entiende que los mismos no suponen prestación del consentimiento: STSJ de Madrid de 21 de noviembre de 2001. En el caso enjuiciado por esta sentencia aparecía un mensaje en la pantalla del ordenador que rezaba lo siguiente: *“La utilización del presente sistema podrá ser objeto de supervisión y registro por razones administrativas o de seguridad. Todo usuario del presente sistema consiente expresamente tal supervisión”*.

⁶⁴ VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales...*, op. cit., pág. 113.

⁶⁵ VEGAS TORRES, J., *Idem.*, pág. 114.

⁶⁶ El caso analizado en esa sentencia versaba sobre un reconocimiento médico al que un trabajador se había sometido voluntariamente pero sin haber sido previamente informado de que se iba a analizar un hipotético consumo de estupefacientes. El TC otorgó amparo por considerar que se había vulnerado el derecho a la intimidad del trabajador por haberse invadido *“la esfera privada de la recurrente sin contar con habilitación legal para ello y sin consentimiento eficaz de la titular del derecho, actuando sin autorización sobre ámbitos que exigían una información expresa y previa al consentimiento”*.

⁶⁷ VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales...*, op. cit., pág. 114.

⁶⁸ VEGAS TORRES, J., *Idem.*, *ibídem*.

puesto de trabajo no cabrá entender que aquel prestó su consentimiento para acceder a datos pertenecientes al ámbito privado y personal que pudiese contener el equipo ni, mucho menos, a que si la intervención técnica de que se tratare desvelara que el ordenador contiene ese tipo de datos, se utilizaren los mismos con fines disciplinarios, siendo en este contexto en el que hay que situar la argumentación efectuada por la STS (Sala IV) de 26 de septiembre de 2007 excluyendo que la intervención en el ordenador del trabajador para eliminar un virus informático amparase el acceso a datos privados y la ulterior adopción de medidas de carácter disciplinario respecto de aquel.

Por lo demás, entendemos que el consentimiento dado por el trabajador a la investigación de su ordenador ha de ser expreso, habiendo de revestir el mismo la forma escrita⁶⁹ y estar basado en una información previa plena y veraz acerca del alcance y la finalidad de aquella y no exceder la misma en ningún caso de dicho alcance ni desviarse de la finalidad referida. Si se cumplen estos requisitos, el consentimiento dado por el trabajador excluiría una hipotética lesión del derecho a la intimidad personal.

No obstante, hemos de señalar que la STC 196/2004, de 15 de noviembre, establece que la Constitución no prescribe la forma escrita como requisito para la validez del consentimiento, añadiendo, por lo demás, que aquélla no excluye la eficacia del consentimiento verbal o la de la realización de actos concluyentes que manifiesten la voluntad del sujeto afectado, si bien la posterior STC 209/2007, de 24 de septiembre, determina que la falta de oposición, salvo en circunstancias excepcionales, no se considera suficiente para entender prestado eficazmente el consentimiento⁷⁰.

A la vista de cuanto antecede, la pregunta que hemos de hacernos es: ¿cabe la posibilidad de inferencias justificadas en la intimidad del trabajador en los supuestos de investigación del ordenador de la empresa?

De lo expuesto hasta ahora conviene señalar que resulta de dudosa legalidad que, en ausencia de instrucciones de uso y control de los medios informáticos comunicadas previamente a los trabajadores de modo expreso, pueda invocarse exitosamente la doctrina de la modulación de los derechos fundamentales para justificar hipotéticas inferencias en el derecho a la intimidad de los trabajadores por parte del empresario.

En este sentido, la doctrina jurisprudencial mayoritaria considera que en ningún caso están justificadas las inferencias en la intimidad de los empleados por parte del empresario, de modo que la única posibilidad de evitar que la investigación de los medios informáticos que la empresa pone a disposición del trabajador conduzca a una hipotética tacha de ilicitud de la prueba por vulnerar el derecho a la

⁶⁹ En sentido contrario, VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales...*, op. cit., pág. 116, que entiende que el consentimiento “puede ser expreso o tácito sin estar sujeto el expreso a especiales requisitos de forma, pudiendo prestarse tanto por escrito como verbalmente”.

⁷⁰ La STC 209/2007, de 24 de septiembre, se refiere al consentimiento prestado para la entrada en el domicilio. No obstante, el criterio que manifiesta ha de entenderse, asimismo, aplicable al consentimiento dado para acceder a datos personales dada la existencia de una clara identidad de razón.

intimidad personal consistiría en la modulación del juego de este derecho fundamental mediante el establecimiento de reglas de uso y control de los mismos conocidas por los trabajadores⁷¹. Argumento que, por lo demás, se ve refrendado por la dicción del art. 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

A ello se ha de añadir que, en clave europea, el TEHD⁷² ha señalado que se habrán de justificar expresamente los motivos para establecer medidas de vigilancia (por lo que entendemos que aquellos habrán de ir más allá de la genérica alusión al poder de control del empresario del art. 20.3 ET), debiendo concretarse en motivos reales y precisos, estableciéndose la necesidad de información previa al trabajador acerca de la vigilancia de su correspondencia electrónica y otro tipo de comunicaciones, así como de la concreta puesta en marcha de las medidas de control, lo cual implica la necesidad de que dicha información haya de ser previa a la efectiva implantación de las medidas de vigilancia y ser, por lo demás, expresa y precisa (*“the notification should normally be clear about the nature of the monitoring and be given in advance”*, dice expresamente la STEDH de 5 de septiembre de 2017, caso Barbulescu c. Rumanía), adoptando el TEDH como referencia principal la normativa sobre protección de datos.

3 EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

3.1 Su Autonomía Frente al Derecho a la Intimidad

1. La protección del derecho a la intimidad se ve acompañada por otro derecho fundamental, cual es el derecho a la autodeterminación informativa, que implica el consentimiento y control de la utilización de datos personales⁷³. Este derecho pretende garantizar a la persona un poder de disposición y control sobre sus datos personales, así como sobre su uso y destino con el objetivo de impedir su tráfico ilícito y/o lesivo para su dignidad y derechos, no reduciéndose el mismo únicamente a datos íntimos, sino que abarca cualquier tipo de dato personal cuyo conocimiento por terceros pueda afectar a sus derechos, sean o no fundamentales⁷⁴. No obstante, hemos de señalar que el derecho a la protección de datos excede al derecho a la intimidad, pues su ámbito instrumental de aplicación no solo está referido al ejercicio de este derecho, sino también al de otros derechos fundamentales, siendo, pues, el derecho a la protección de datos un derecho específico y distinto al derecho a la intimidad.

⁷¹ VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales...*, op. cit., pág. 117.

⁷² STEDH de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía).

⁷³ OLLERO TASSARA, A., ¿Son jurídicos los derechos humanos?, *Revista SCIO*, nº 4, 2009, págs. 141-142.

⁷⁴ STC 292/2000, de 30 de noviembre, FJ 4º.

Ello se debe a que, como el propio TC reconoce en su sentencia 292/2000, de 30 de noviembre –que resuelve recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra determinados preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal–, tanto el derecho a la intimidad o el derecho a la vida privada, como otros derechos fundamentales, tienen una dimensión positiva que reclama un control sobre los datos relativos a la propia persona, sobre su uso y destino con el fin de impedir su trato ilícito y lesivo para la dignidad de la persona cuyos datos se tratan. De ahí, como señala la sentencia referida, la singularidad y especificidad del derecho a la protección de datos, cuyo objeto es más amplio que el del derecho a la intimidad, ya que aquel extiende sus garantías no solo a la intimidad, sino a cualquier ámbito de los bienes de la personalidad, que puedan verse vulnerados con el uso inadecuado de estos datos.

Por ello, todo dato de carácter personal que identifique o permita la identificación de una persona debe ser protegido por el derecho a la protección de datos⁷⁵, pues dichos datos pueden servir para la confección de su perfil ideológico, económico, sexual, racial o de cualquier otra índole que, usado en ciertas condiciones o circunstancias, puede llegar a constituir una amenaza para el individuo, por lo que este derecho otorga a su titular un haz de facultades que le confieren la potestad de ejercer un poder de disposición y control sobre sus datos personales, facultándolo para decidir cuáles de estos datos proporciona a un tercero, ya sea el Estado o un particular, pudiendo conocer aquel en todo momento quién posee esos datos personales y para qué, así como oponerse a esa posesión o uso⁷⁶.

De este modo, aunque el derecho a la protección de datos tiene sus propias peculiaridades que lo convierten en un derecho con un contenido específico y con un sistema de protección propio, dichas características coexisten con la función de garantía instrumental de otros derechos en razón de los riesgos de lesión de determinados derechos fundamentales que, por ejemplo, el tratamiento de datos personales a través de la introducción de las nuevas tecnologías pueden producir en sus titulares⁷⁷.

En cuanto a los caracteres del derecho a la protección de datos, señalar que se trata de un derecho fundamental relacionado con la vida privada, pero independiente y distinto de esta, tiene carácter universal, está vinculado a la dignidad humana y, por

⁷⁵ A este respecto, la AEPD ha señalado que si es posible deducir de las listas que contienen los resultados obtenidos por productividad, proporcionadas por el empleador a los trabajadores y que son publicadas a través del tablón de anuncios o en Internet, la identidad de los empleados, sin realizar para ello esfuerzos desproporcionados, deben ser elaboradas y difundidas únicamente con el consentimiento de los trabajadores involucrados, salvo que el Comité de Empresa se pronuncie considerando estas medidas como controles que efectúa el propio empresario a su trabajador al amparo del art. 20.3 ET, en cuyo caso la cesión vendría amparada en el mencionado artículo. *Vid.* Agencia Española de Protección de Datos, *Informe N° 0529-2009: Comunicaciones de la productividad de los trabajadores a otros trabajadores*, AEPD, Madrid, 2009. En <http://www.agpd.es>.

⁷⁶ APARICIO ALDANA, R. K., *Derecho a la intimidad y a la propia imagen...*, *op. cit.*, pág. 88.

⁷⁷ DESDENTADO BONETE, A. y MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012, pág. 81.

tanto, de titularidad de las personas físicas, sean nacionales o extranjeras⁷⁸, que tiene por objeto garantizar la libertad del individuo en relación a su autodeterminación respecto del tratamiento de sus datos personales por terceros y que presenta como contenido un conjunto de facultades consistentes, en su mayoría, en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos clasificables como acceso, rectificación, cancelación u oposición⁷⁹.

Por ello, el uso empresarial de los datos personales de los empleados ha de ir acompañado de un control, por parte de los trabajadores, sobre su uso, más aún cuando, con el surgimiento de las nuevas tecnologías, los empresarios, para facilitar sus actividades de gestión del personal, cuentan con soportes informáticos que les facilitan almacenar gran cantidad de datos, cruzarlos y tratar información, lo que les permite ir más allá de lo que el propio dato revela, haciendo más sencilla la labor de entrelazar datos no íntimos o que aislados no tengan mayor importancia, pero que entrecruzados pueden ofrecer un retrato de la personalidad o de la historia del individuo que este tiene derecho a mantener en reserva⁸⁰.

El derecho a la protección de datos no es, por lo demás, un derecho absoluto, sino limitado⁸¹ (art. 52.1 CDFUE y art. 8 CEDH)⁸², estando sujeto a limitaciones de origen legal por norma con rango de ley accesible y previsible. Limitaciones que, por otro lado, han de responder a una necesidad imperiosa, debiendo ser adecuadas y proporcionadas al logro de ese propósito, en definitiva, indispensables en una sociedad democrática⁸³. Entre tales limitaciones la jurisprudencia ha considerado legítimas la seguridad del Estado⁸⁴, la persecución de infracciones penales o la distribución equitativa del sostenimiento del gasto público, entre otras.

3.2 Sus Diferencias Respecto al Derecho a la Intimidad

La protección de datos personales ostenta, en el ordenamiento jurídico español, la naturaleza de derecho fundamental. Así, el Tribunal Constitucional estableció la existencia de este derecho fundamental en diferentes sentencias -desde

⁷⁸ SSTC 292/2000, de 30 de noviembre, FJ 4º y 17/2013, de 31 de enero, FJ 3º.

⁷⁹ PRECIADO DOMENECH, C. H., *El derecho a la protección de datos en el contrato de trabajo*, Thomson Reuters Aranzadi, Pamplona, 2017, pág. 36.

⁸⁰ PÉREZ DE LOS COBOS ORIHUEL, F., *Nuevas tecnologías y relación de trabajo*, Tirant lo Blanch, Valencia, 1990, pág. 73.

⁸¹ SSTJUE de 24 de noviembre de 2011 (caso Asociación Nacional de Establecimientos Financieros de Crédito, Asuntos C-468/10 y C-469/10) y de 9 de noviembre de 2010 (caso Volker und Markus Schecke GbR y Hartmut Eifert c. Land Hessen, Asuntos acumulados C-92/09 y C-93/09, de 9 de noviembre de 2010).

⁸² Sobre las limitaciones del derecho en el nuevo Reglamento *vid.* Art. 24 Reglamento 679/2016, que se corresponde con el art. 13 de la Directiva 95/46.

⁸³ SSTEDH de 26 de marzo de 1985 (caso X e Y c. Países Bajos), de 26 de marzo de 1987 (caso Leander c. Suecia), de 7 de junio de 1989 (caso Gaskin c. Reino Unido) y de 25 de febrero de 1983 (caso Funke c. Francia).

⁸⁴ STEDH de 26 de marzo de 1987 (caso Leander c. Suecia).

la STC 254/1993, de 20 de julio, hasta la mencionada STC 292/2000, de 30 de noviembre-, configurándolo como un derecho de naturaleza instrumental de textura abierta que se relaciona con el entero sistema de derechos fundamentales⁸⁵ y fundamentándolo en el art. 18.4 de la CE, siendo en esta última resolución en la que se perfilan las características más importantes de su régimen jurídico, distinguiéndolo del derecho a la intimidad en base a tres criterios diferenciales: diferencias en la función, en el objeto y en el contenido⁸⁶.

Por otro lado, el Tribunal Constitucional establece que tanto el derecho a la intimidad como el derecho a la protección de datos no son derechos incompatibles, si bien los mismos presentan perfiles diferentes, residiendo la peculiaridad del derecho a la protección de datos respecto del derecho a la intimidad en su distinta función, ya que si bien éste protege al individuo frente a cualquier acto de injerencia que pudiera efectuarse en aquellos aspectos de su vida personal y familiar que desee excluir de intromisiones de terceros en contra de su voluntad, aquel, por el contrario, lo que persigue es garantizar al individuo un poder de disposición y control sobre sus datos personales, su uso y destino, con la finalidad de impedir su tráfico ilícito y/o lesivo para su dignidad⁸⁷.

Asimismo, la distinción que se advierte obedece también a la especialidad del objeto que protege, el cual es más amplio en el caso de la protección de datos habida cuenta de que el objeto de protección no se circunscribe solamente a los datos más íntimos o privados del individuo, sino a cualquier tipo de dato de carácter personal, íntimo o no, cuyo conocimiento o uso por terceros pudiere afectar a sus derechos, sean o no estos fundamentales.

Por último, existe también una importante diferencia en cuanto al elenco de facultades que atribuyen ambos derechos. Así, mientras el derecho a la intimidad confiere a su titular el poder jurídico de imponer a terceros un deber de abstención de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo conocido, el derecho a la protección de datos atribuye a aquel un haz de facultades que engloba diversos poderes jurídicos cuyo ejercicio impone, a su vez, a terceros deberes jurídicos que no se incluyen en el anterior⁸⁸.

Obsérvese que no estamos hablando tanto de la privacidad de los ciudadanos en su esfera de intimidad personal frente a terceros o en sus comunicaciones, sino ante las garantías constitucionales de que sus datos personales, integrados en cualquier soporte no puedan ser destinados, sin su consentimiento, a fines distintos de aquellos para los que fueron revelados. Sin embargo, en la práctica –como la experiencia judicial y constitucional pone en evidencia– no siempre resulta fácil

⁸⁵ MARTÍNEZ MARTÍNEZ, R., ¿Minusvaloramos la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales?, *La Ley*, nº 9329, Sección Tribuna, 3 de enero de 2019.

⁸⁶ LÓPEZ JIMÉNEZ, D., “Los Códigos Tipo como instrumento para la protección de la privacidad en el ámbito digital: apreciaciones desde el Derecho español”, en *Estudios Constitucionales*, año 11, nº 2, 2013, Centro de Estudios Constitucionales de Chile Universidad de Talca, pág. 587.

⁸⁷ LÓPEZ JIMÉNEZ, D., “Los Códigos Tipo como instrumento para la protección de la privacidad...”, *op. cit.*, pág. 588.

⁸⁸ LÓPEZ JIMÉNEZ, D., *Idem.*, *Ibidem.*

diferenciar en el mundo laboral, cuando existen grabaciones, los límites entre los apartados 1 y 4 del art. 18 CE, estándose, generalmente, en estos casos ante un concurso real de derechos.

En efecto, un registro videográfico en un vestuario afecta, sin duda, al derecho a la intimidad en forma absoluta. De similar manera, una grabación en el puesto de trabajo también puede hacerlo –tal y como se desprende de la STC 98/2000, de 10 de abril–. Ahora bien, si como es la práctica habitual, las imágenes así obtenidas se almacenan en una base de datos, aparecen también las dudas de la posible afectación al derecho a la protección de datos, como antes se ha indicado⁸⁹.

3.3 Afectación del Derecho a la Protección de Datos Personales

Para poder determinar la naturaleza de la injerencia en el derecho a la protección de datos derivados de la captación de imágenes y sonidos mediante videocámaras resulta necesario la reunión de todos los elementos del supuesto de hecho de la norma constitucional. Es decir, habrá que examinar si los dispositivos de videovigilancia recogen datos de carácter personal protegidos por el derecho fundamental a la protección de datos, de modo que la relevancia iusfundamental de la videovigilancia dependerá del tipo de dispositivo utilizado⁹⁰.

Los datos amparados por el derecho a la protección de datos frente a la informática son todos aquellos que identifiquen o permitan identificar a una persona y puedan valer para confeccionar su perfil ideológico, sexual, racial, económico, social o de cualquier otra índole o puedan servir para cualquier otra utilidad que constituya una amenaza para el individuo⁹¹. La clave está, pues, en la identificación o identificabilidad de la persona, de modo que si las grabaciones de imágenes y los sonidos que captan los dispositivos de videovigilancia identifican o permiten identificar a las personas constituirán datos de carácter personal y se estará penetrando en el ámbito de protección del derecho a la protección de datos personales. Por el contrario, si las imágenes captadas no permitieren identificar personas concretas, la utilización de las cámaras está fuera del ámbito de protección constitucional del citado derecho.

Pero la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, requiere algo más para considerar que una grabación de imágenes y sonidos contiene datos de carácter personal en el sentido de la legislación de protección de datos. Así, según su art. 2.1, lo dispuesto en sus Títulos I a IX y en los arts. 89 a 94 de se aplicará a cualquier tratamiento,

⁸⁹ FALGUERA BARÓ, M. A., “Nuevas tecnologías y trabajo (II): perspectiva constitucional”, *Trabajo y Derecho*, núm. 21, septiembre 2016, pág. 45. Es conveniente indicar que esa base de datos con imágenes supone la creación de un “fichero de datos” (art.3.b) LOPD y, por tanto, sometida a la LOPD. Respecto a la consideración de una imagen como dato y la transmisión de imágenes de trabajadores en su lugar de trabajo mediante una webcam e internet, ver la SAN de 24 de enero de 2003, Sala de lo Contencioso. Asimismo, para una mejor comprensión del problema, véase NAVARRO MARCHANTE, V. J., *El derecho a la información audiovisual de los juicios*, CEPCC, 2011, pág. 142.

⁹⁰ ARZOZ SANTISTEBAN, X., *Videovigilancia, seguridad ciudadana y derechos fundamentales*, Civitas, Madrid, 2010, pág. 137.

⁹¹ STC 254/1993, de 20 de julio, FJ 5º.

total o parcialmente automatizado, de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

Y, por su parte, el art. 4.6 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) define el concepto de “fichero” como todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica, de manera que el criterio decisivo es el de conjunto organizado registrado en un soporte físico, por lo que la obtención de imágenes mediante sistemas de grabación digital, bajo el control de un ordenador, puede considerarse tratamiento automatizado en el sentido del art. 2.1 de la Ley Orgánica 3/2018, de 5 de diciembre.

En el ámbito de la videovigilancia empresarial, la AEPD ha interpretado que las grabaciones tomadas en el lugar de trabajo constituyen un conjunto organizado porque sabiendo el horario de trabajo de una persona se puede acceder a las imágenes referidas a la persona en cuestión. En este ámbito, las imágenes captadas se pueden relacionar fácilmente con personas determinadas, de modo que la captación de la imagen de los trabajadores a través de cámaras de videovigilancia constituye un dato de carácter personal ya que toda la información captada concierne a la persona y proporciona información sobre la imagen personal de esta, su lugar de captación y la actividad desarrollada por aquel a quien la imagen se refiere, por lo que la misma se encuentra sometida a las prescripciones previstas en la legislación sobre protección de datos en la medida en que sea objeto de tratamiento⁹².

Dado que las actividades de videovigilancia laboral caen dentro de la órbita de las facultades de control del empresario reconocidas a este en el art. 20.3 ET, la captación y tratamiento de imágenes de los trabajadores para controlar el cumplimiento de su prestación laboral serán lícitos, de conformidad con lo dispuesto en el art. 6.1 del Reglamento Europeo de Protección de Datos, si se cumple al menos una de las siguientes condiciones:

- a) Que el interesado hubiere prestado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.
- b) Que el tratamiento resultare necesario para la ejecución de un contrato en el que el interesado fuese parte o para la aplicación, a petición de este, de medidas precontractuales.
- c) Que el mismo fuera necesario para cumplir una obligación legal aplicable al responsable del tratamiento.
- d) Que resultara necesario en orden a la protección de intereses vitales del interesado o de otra persona física.
- e) Que fuese necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

⁹² DESDENTADO BONETE, A. y MUÑOZ RUIZ, A. B., *Control informático, video vigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012, pág. 62.

- f) Que el tratamiento deviniera necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

No obstante, lo dispuesto en la letra f) no será de aplicación al tratamiento que realicen las autoridades públicas en el ejercicio de sus funciones.

Por su parte, el art. 6.3 de la Ley Orgánica 3/2018, de 5 de diciembre, al hablar del tratamiento basado en el consentimiento del afectado, impide supeditar la ejecución de un contrato al consentimiento por parte del afectado para tratar sus datos personales para finalidades que no tengan relación directa con el desarrollo de la relación contractual, al disponer expresamente que *“no podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual”*.

5. Ahora bien, el hecho de que pueda no resultar necesario el consentimiento expreso de los trabajadores acerca de la videovigilancia, ello no quiere decir que el empresario no deba informar expresamente a los mismos de la instalación de los medios de control en la empresa con el fin de evitar vulnerar derechos fundamentales. A tal efecto, la AEPD ha dejado claro que lo importante es que el trabajador esté debidamente informado acerca de la finalidad de la vigilancia, al tiempo que sugiere que se aclare cuál es la política de la empresa acerca de la utilización de los medios electrónicos, qué conductas están autorizadas y cuáles no y qué herramientas de inspección se van a utilizar⁹³. En esta misma línea, si se trata de la instalación de cámaras de videovigilancia, es necesario que en las zonas video vigiladas se coloque un distintivo informativo, poniéndose en conocimiento de los representantes de los trabajadores, sin que puedan ser utilizados para fines distintos de los declarados.

En este sentido, el art. 89 de la Ley Orgánica 3/2018, de 5 de diciembre, establece que el empresario podrá tratar las imágenes obtenidas a través de sistemas de cámaras de videovigilancia para el ejercicio de las funciones de control previstas en el art. 20.3 ET siempre que las mismas se ejerzan dentro del marco legal y con los límites inherentes al mismo, debiendo el empleador informar con carácter previo y de forma expresa a los trabajadores y, en su caso, a sus representantes, acerca de esta medida.

4 CONCLUSIONES

- a) Los derechos fundamentales no pueden ser ignorados por el clausulado de un contrato de trabajo, ejerciendo los derechos fundamentales en el ámbito de la relación laboral una función equilibradora entre trabajador y empresario.

⁹³ Informe Jurídico 0247/2008: Acceso por el empresario al correo electrónico de los trabajadores.

- b) El derecho fundamental a la intimidad despliega toda su eficacia también en el seno de las relaciones jurídico laborales, si bien no se trata de un derecho ilimitado o absoluto, sino que el mismo puede ceder ante intereses constitucionales.
- c) El ordenador se incluye entre los medios, propiedad de la empresa, que esta pone a disposición del trabajador para que los utilice en el cumplimiento de su prestación de trabajo, de modo que ese uso cae bajo la órbita del poder de vigilancia y control del empresario (STS 26 septiembre 2007).
- d) La doctrina posterior a la STS 26 septiembre 2007 ha permitido la prohibición absoluta del uso privado del ordenador, posibilitando un control empresarial completo de su utilización por parte del trabajador (v. gr. STS de 6 octubre 2011 y STC 170/2013, de 7 octubre), si bien esta posición ha quedado en entredicho a raíz de la STEDH de 5 de septiembre de 2017 en el caso *Barbulescu c. Rumanía*, que proscribe la reducción a cero del ejercicio de los derechos fundamentales del trabajador en el seno de la empresa.
- e) Constituye una carga para el empresario el establecimiento de reglas de uso y control que sean conocidas expresamente por los trabajadores en el sentido de que, si no lo hiciere, no podrá obtener pruebas lícitas en orden a la defensa ante los tribunales de justicia de las medidas disciplinarias que pudiera adoptar.
- f) El derecho a la protección de datos es un derecho fundamental relacionado con la vida privada, pero independiente y distinto de esta, que tiene carácter universal y está vinculado a la dignidad humana y, por tanto, de titularidad de las personas físicas, sean nacionales o extranjeras, que tiene por objeto garantizar la libertad del individuo en relación a su autodeterminación respecto del tratamiento de sus datos personales por terceros.

BIBLIOGRAFÍA

APARICIO ALDANA, R. K., *Derecho a la intimidad y a la propia imagen en las relaciones jurídico laborales*, Thomson Reuters Aranzadi, Cizur Menor, Pamplona, 2016.

ARZOZ SANTISTEBAN, X., *Videovigilancia, seguridad ciudadana y derechos fundamentales*, Civitas, Madrid, 2010.

CARRILLO LÓPEZ, M., “Los ámbitos del derecho a la intimidad en la sociedad”, en *El derecho a la privacidad en un nuevo entorno tecnológico*, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional, Centro de Estudios Políticos y Constitucionales, Madrid, 2016.

DESDENTADO BONETE, A. y MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012.

FABREGAT MONFORT, G., “El control empresarial de los trabajadores a través de las nuevas tecnologías: algunas ideas clave”, *Trabajo y Derecho*, nº 5, 2015.

FALGUERA BARÓ, M. A., “Nuevas tecnologías y trabajo (II): perspectiva constitucional”, *Trabajo y Derecho*, núm. 21, septiembre 2016.

GALLARDO MOYA, R.: “El derecho fundamental a la protección de datos y la videovigilancia empresarial”, *Revista de Derecho Social*, nº 62.

GARCÍA VITORIA, I., “La protección de datos como eje de la jurisprudencia del Tribunal de Estrasburgo sobre la privacidad del trabajador y el control empresarial”, en <<http://eapc-rcdp.blog.gencat.cat>>.

GOERLICH PESET, J. M^a., “Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas”, en *El derecho a la privacidad en un nuevo entorno tecnológico, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016.

GUERRA RODRÍGUEZ, L., “Ejercicio del poder de control a través de cámaras de video vigilancia: análisis de la doctrina constitucional”, *Trabajo y Derecho* 29/2017 (mayo), nº 29 de 1 de mayo de 2017.

JIMÉNEZ PÉREZ, A., “El derecho a la intimidad en la jurisprudencia constitucional y convencional: el Tribunal Constitucional Español, el Tribunal Europeo de Derechos Humanos y la Corte Interamericana de Derechos Humanos”, en *El derecho a la intimidad. Nuevos y viejos debates*, Dykinson, Madrid, 2017.

LÓPEZ JIMÉNEZ, D., “Los Códigos Tipo como instrumento para la protección de la privacidad en el ámbito digital: apreciaciones desde el Derecho español”, en *Estudios Constitucionales*, año 11, nº 2, 2013, Centro de Estudios Constitucionales de Chile Universidad de Talca.

MACAVILCA ROMÁN, Z., “El derecho a la intimidad y las nuevas tecnologías. El derecho a la intimidad en el contexto de las nuevas tecnologías de comunicación e información”, en *El derecho a la intimidad. Nuevos y viejos debates*, Dykinson, Madrid, 2017.

MARTÍNEZ MARTÍNEZ, R., ¿Minusvaloramos la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales?, *La Ley*, nº 9329, Sección Tribuna, 3 de enero de 2019.

MIERES MIERES, L. J., “La protección constitucional de los derechos a la intimidad y a la propia imagen en las relaciones laborales: una visión desde la jurisprudencia constitucional”, *RVAP*, núm. 99-100 (Especial “Demetrio Loperena Rota, *In memoriam*), mayo – diciembre, 2014.

MIERES MIERES, L. J., *Intimidación personal y familiar. Prontuario de jurisprudencia constitucional*, Aranzadi, Navarra, 2002, pág.23.

NAVARRO MARCHANTE, V. J., *El derecho a la información audiovisual de los juicios*, CEPC, 2011.

OLLERO TASSARA, A., ¿Son jurídicos los derechos humanos?, *Revista SCIO*, nº 4, 2009.

PÉREZ DE LOS COBOS ORIHUEL, F., *Nuevas tecnologías y relación de trabajo*, Tirant lo Blanch, Valencia, 1990.

PONCE RODRÍGUEZ, S., “El poder de control empresarial sobre los medios informáticos puestos a disposición del trabajador. Sentencia del Tribunal Supremo de 26 de septiembre de 2007”, *Revista Actualidad Jurídica Uría Menéndez*, núm. 19, enero-abril 2008.

PRECIADO DOMENECH, C. H., *El derecho a la protección de datos en el contrato de trabajo*, Thomson Reuters Aranzadi, Pamplona, 2017.

RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M., “Derecho a la intimidad del trabajador y contrato de trabajo”, en *Diario La Ley*, núm. 6033, de 4 de junio de 2004.

VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa*, Universidad Rey Juan Carlos, Madrid, 2011.