ISSN: 1696-3083, Revista Galega de Dereito Social -2ª ET- (8,2019), pp. 85-127
http://www.revistagalegadedereitosocial.gal

AUTODETERMINACIÓN INFORMATIVA: UN DERECHO EN ALZA

CARMEN SÁNCHEZ TRIGUEROS
Catedrática de Derecho del Trabajo y de la Seguridad Social
Universidad de Murcia
carmenst@um.es

MARÍA ELISA CUADROS GARRIDO
Abogada. Profesora Asociada (acred. Ayudante Doctora)
Universidad de Murcia
mariaelisa.cuadros@um.es

RESUMEN
La protección de datos es un derecho fundamental que ha permanecido larvado, pero a partir de la STC 29/2013 ha emergido con fuerza, sometiéndose a diversos vaivenes jurisprudenciales que al final han venido a consagrarlo como un derecho más potente que la propia intimidad o el secreto de las comunicaciones, imponiendo sus principios de actuación mucho más exigentes y formalistas que lo que habían servido hasta ahora para limitar otros derechos fundamentales. Su concepción está en pleno crecimiento por lo que no es posible cerrar su delimitación, y ello genera problemas de interpretación y constante readaptación.
Palabras clave: Libertad informática; derechos digitales; protección de datos.

ABSTRACT
Data protection is a fundamental right that has remained latent and since STC 29/2013 it has emerged with strength, submitting to various jurisprudential swings that in the end have come to consecrate it as a more powerful right than the privacy or secrecy of communications, imposing its principles of action much more demanding and formalist than what had served until now to limit other fundamental rights. It is not risky to affirm that its conception is in full growth so it is not possible to close its delimitation, and this

Recibido: 12/05/2019; Aceptado: 10/06/2019

generates problems of interpretation and continuous readjustment.
Keywords: Computer freedom; digital rights; Data Protection.

RESUMO
A protección de datos é un dereito fundamental que permaneceu larvado, pero a partir da STC 29/2013 emerxeu con forza, someténdose a diversos vaivéns xurisprudenciais que ao final viñeron a consagralo como un dereito máis potente que a propia intimidade ou o secreto das comunicacións, impoñendo os seus principios de actuación moito máis esixentes e formalistas que os que serviran ata agora para limitar outros dereitos fundamentais. A súa concepción está en pleno crecemento polo que non é posible pechar a súa delimitación, e iso xera problemas de interpretación e constante readaptación.
Palabras crave: Liberdade informática; dereitos dixitais; protección de datos.

SUMARIO
1. **DELIMITACIÓN**. 1.1. CONCEPTO. 1.1.1. DELIMITACIÓN FRENTE AL DERECHO A LA INTIMIDAD. 1.1.2. DELIMITACIÓN FRENTE AL DERECHO AL SECRETO DE LAS COMUNICACIONES. 1.2. UN DERECHO EN EVOLUCIÓN. 2. **EL ART. 8 DEL CONVENIO EUROPEO DE DERECHOS HUMANOS**. 2.1. LOS CASOS HALFORD Y COPLAND. 2.2. EL CASO BARBULESCU. 2.3. EL CASO LÓPEZ RIBALDA. 3. **EL REGLAMENTO GENERAL DE DATOS**. 3.1. ÁMBITO DEL RGD. 3.2. DERECHO AL OLVIDO. 3.3. DERECHO A LA PORTABILIDAD DE LOS DATOS. 4. **LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y GARANTÍA DE DERECHOS DIGITALES**. 4.1. IDEA GENERAL. 4.2. USOS E DISPOSITIVOS DIGITALES EN EL ÁMBITO LABORAL. 4.3. DERECHO A LA DESCONEXIÓN DIGITAL EN EL ÁMBITO LABORAL. 4.4. DISPOSITIVOS DE VIDEOVIGILANCIA Y DE GRABACIÓN DE SONIDOS. 5. **EVOLUCIÓN DE LA JURISPRUDENCIA CONSTITUCIONA**L. 5.1. PRIMERA ETAPA. 5.2. SEGUNDA ETAPA. 5.3. TERCERA ETAPA. 5.4.

CUARTA ETAPA. 5.5. QUINTA ETAPA. 5.6. SEXTA ETAPA. 6. **REFLEXIONES CONCLUSIVAS**. 7. **BIBLIOGRAFÍA**.

1. DELIMITACIÓN

1.1. CONCEPTO

Nuestro legislador constitucional fue pionero al reconocer el derecho fundamental a la protección de datos personales, pero su alcance e interpretación en el sistema español como derecho fundamental[1] es una creación jurisprudencial[2], en buena medida obra de nuestro Tribunal Constitucional[3].

El perfil del derecho analizado es marcadamente formalista, ya que garantiza a la persona el control activo de las informaciones que le afectan, y el derecho a no ser instrumentalizado a través del conocimiento adquirido de aspectos de su personalidad, en la medida en que supone ser informado de quién posee sus datos personales, a qué uso se están sometiendo y el derecho a oponerse, en su caso, a una posesión ilegítima o uso ilícito; es la potestad de control sobre el uso de los datos propios.

[1] El artículo 18.4 CE, establece en puridad, un mandato al legislador y no un derecho fundamental en sentido propio, así dispone lo siguiente: *la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno uso de sus derechos*. La redacción del precepto constitucional no es afortunada, ya que limitar el uso de la informática, además de poco factible, es poco deseable, cosa distinta, que es sin duda lo que el constituyente quiso decir, es *poner coto* a los eventuales abusos en el empleo de las nuevas tecnologías. El mandato constitucional es, sin duda, una garantía para la plena eficacia de otros derechos como son el honor y la intimidad. En este sentido, sobre el legislador pesa el deber de regular el tratamiento de datos de manera que dicha actividad se realice de forma respetuosa con los derechos fundamentales.

[2] Las vulneraciones a la autodeterminación informativa por parte de los particulares tienen relevancia constitucional y por consiguiente también se consideran violaciones del artículo 18.4 CE y esto significa, en la práctica que son susceptibles de protección vía recurso de amparo.

[3] Así, el Tribunal Constitucional ha amparado a los trabajadores frente a la utilización empresarial no justificada de información sobre afiliación sindical (STC 11/1998, de 12 de febrero) o frente a la creación por el empresario sin el consentimiento de los afectados de un fichero sobre absentismo con baja médica (STC 202/1999 de 8 de noviembre).

El TC viene a considerar este derecho[4] como *una facultad de control sobre los datos relativos a la propia persona*, añadiendo que la llamada *libertad informática*[5] es el derecho a controlar el uso de los mismos datos insertos en un programa informático, *habeas data*[6], y comprende la oposición del ciudadano a que determinadas informaciones personales sean utilizadas para fines distintos del legítimo que justificó su obtención.

Para establecer un correcto análisis y delimitación hemos de mencionar los otros dos derechos que en materia de control de TICs pueden resultar afectados; el derecho a la intimidad y el derecho al secreto de las comunicaciones.

1.1.1. Delimitación frente al derecho a la intimidad

Según reiterada jurisprudencia constitucional, el derecho a la intimidad personal, en cuanto derivación de la libertad y dignidad de la persona, art. 10.1 CE, implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario según las pautas de nuestra cultura, para mantener una mínima calidad de vida humana. A fin de resguardar ese espacio reservado, este derecho confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido (STC 196/2004, de 15 de noviembre). Por lo tanto, *el atributo más importante de la intimidad, como núcleo central de personalidad, es la facultad de exclusión de los demás de la abstención de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos*

[4] En este punto, SEMPERE NAVARRO y SAN MARTÍN MAZZUCCONI advierten que el Tribunal Constitucional se *afana en deslindar* la libertad informática respecto del derecho a la intimidad, pero tácitamente, reconoce que la escisión no puede ser absoluta, porque el derecho a la protección de datos comprende el derecho a la intimidad, aunque lo exceda. *Vid*. SEMPERE NAVARRO, A. V. y SAN MARTÍN MAZZUCCONI, C.: *Nuevas tecnologías y Relaciones Laborales, Aranzadi, 2002,* pág. 120.

[5] STC 202/1999 de 8 noviembre (RTC 1999\202).

[6] Según la RAE el derecho a la propia intimidad informática, que confiere a su titular un derecho de control sobre los datos (acceso, rectificación y cancelación de estos), interviniendo el Estado en su protección con agencias o comisarios para la protección de los datos.

intrusiva, como a la divulgación ilegítima de estos datos (STC 142/1993, de 22 de abril).

1.1.2. Delimitación frente al derecho al secreto de las comunicaciones

El secreto de las comunicaciones, expresamente proclamado en el art. 18.3 CE, tiene un significado instrumental respecto de la libertad, pues se garantiza el secreto de las comunicaciones para que éstas puedan desarrollarse con libertad. Así podemos realizar una serie de precisiones:

- Solo la comunicación que ha de valerse de algún medio técnico está cubierta por el art. 18.3 CE. No lo está, sin embargo, la directa.
- Se protege el soporte y el contenido.
- El secreto no rige entre los propios comunicantes, y en consecuencia la grabación de la propia conversación no vulnera el secreto de las comunicaciones.

1.2. UN DERECHO EN EVOLUCIÓN

Para cierto sector de la doctrina constitucionalista encabezado por CÓRDOBA CASTROVERDE y DÍEZ PICAZO, el art. 18.4 CE supone un derecho con una tremenda fuerza arrolladora, pues si bien ha permanecido larvado durante un gran lapso de tiempo, actualmente se ha convertido en *un agujero negro que lo absorbe todo y no deja escapar nada de su entorno*. E incluso a la luz de los amplios conceptos de datos personales y tratamiento, estos autores consideran que cualquier acto de comunicación basado en medios automáticos, como las telecomunicaciones, el correo electrónico o las redes sociales, relativo a una persona física, constituye una interferencia putativa tal de este derecho fundamental que requiere de justificación[7].

En parecido sentido, se pronuncian dentro de la doctrina social GARCÍA-PERROTE ESCARTÍN y MERCADER UGUINA al

[7] CÓRDOBA CASTROVERDE, D. y DÍEZ- PICAZO GIMÉNEZ, L. M.: Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico en AA. VV. Asociación de Letrados del Tribunal Constitucional (Coord.): *El derecho a la privacidad en un nuevo entorno tecnológico. XX Jornadas de la Asociación de Letrados del Tribunal Constitucional*, CEPC, 2016, págs. 99-122.

afirmar que la protección de datos comienza a ocupar los espacios de la privacidad imponiendo sus principios de actuación mucho más exigentes y rigurosos que lo que habían servido hasta ahora para limitar el derecho a la intimidad[8]. Llegándose incluso a afirmar que estamos ante un derecho en construcción, de perfiles no completamente acabados, y que por ello mismo no hay que descartar que en un futuro más o menos próximo presente novedades o aspectos que hoy en día pudieran sorprendernos o, cuando menos, que no somos capaces de adivinar[9].

El objeto del derecho fundamental a la protección de datos desde la perspectiva de las relaciones laborales persigue garantizar a la persona un poder de control sobre sus datos personales, su uso y su destino, con el propósito de impedir un tráfico ilícito y lesivo para la dignidad del trabajador afectado. Su concepción abarca cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo pueda afectar a los derechos de la persona, sean o no fundamentales.

Desde una perspectiva laboral, el contrato de trabajo es, sin duda, una zona *particularmente sensible*[10] en orden a las amenazas que para la vida privada de los trabajadores pueden derivar del control de los datos personales, o dadas las características propias de la relación laboral que hacen que existan dificultades y excepciones a la hora de trasplantar el régimen jurídico propio de la protección de datos de carácter personal al ámbito de la empresa.

---

[8] GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, J. R: La protección de datos se come a la intimidad: la doctrina de la sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (caso Bărbulescu v. Rumania; nº 61496/08; Gran Sala), *Revista de Información Laboral*, núm. 10, 2017.

[9] GARCÍA MURCIA, J, y RODRÍGUEZ CARDO, I. A.: La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo*, Revista Española de Derecho del Trabajo*, núm. 216, 2019 (BIB 2019\1432).

[10] El peligro denunciado se multiplica por el desequilibrio de las posiciones de poder en la relación de trabajo, dentro de la cual, el trabajador tiene menor capacidad de resistencia a las pretensiones de control informativo. *Vid*. CUADROS GARRIDO, M.E.: *Trabajadores Tecnológicos y Empresas Digitales*, Aranzadi, 2018, pág. 135.

2. EL ART. 8 DEL CONVENIO EUROPEO DE DERECHOS HUMANOS

2.1. LOS CASOS HALFORD Y COPLAND

La autodeterminación informativa se encuentra de manera implícita dentro de los derechos protegidos por el art. 8[11] del Convenio Europeo para la salvaguardia de los Derechos Humanos y las Libertades Fundamentales (CEDH)[12], y en algunos arranques puntuales de esta doctrina jurisprudencial en los casos *Huvig y Krsuling v. Francia* de 24 de abril de 1.990[13]. Se hace necesario por ello aludir a dos importantes sentencias del Tribunal Europeo de Derechos Humanos, consideradas como *leading case*, en los términos que establecen las SSTDH de 25 de junio de 1997 -caso HALFORD- y de 3 de abril de 2007 –sentencia COPLAND– para valorar la existencia de una lesión del art. 8 del Convenio Europeo para la Protección de los Derechos Humanos; y a través de este ha pasado a formar parte de la jurisprudencia de la Sala IV del Tribunal Supremo y posteriormente de la del Tribunal Constitucional.

El *caso Halford contra el Reino Unido*[14]*,* constituye el primero en el que se llevó a cabo una utilización explícita de la doctrina de la *expectativa de privacidad*[15]. Los hechos que se declararon probados en la sentencia son los siguientes:

---

[11] Artículo 8 sobre el derecho al respeto a la vida privada y familiar, cuya literalidad es la siguiente: «1. Toda persona tiene derecho al respeto a su vida privada y familiar, de su domicilio y de su correspondencia; 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida, que en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás».

[12] Convenio Europeo para la Protección de los Derechos Humanos y las libertades fundamentales hecho en Roma el 4 de noviembre de 1950. Protocolo adicional al Convenio hecho en París el 20 de marzo de 1952.

[13] STDH 24 de abril de 1999 (TEDH 1990, 2).

[14] STDH de 25 de junio de 1997 (TEDH 1997, 37).

[15] El referido criterio podría definirse con la siguiente máxima: un ciudadano no puede ser sometido a una injerencia sobre su privacidad con la que no pudiera contar en términos razonables. Sus antecedentes se encuentran en EEUU y parten de la interpretación dada por la *Supreme Court* a la Cuarta Enmienda de la Constitución Americana, que contempla

- La demandante, llamada Alinson Halford, era inspectora general de la policía británica de Merseyside.
- Antes del proceso ante el TEDH, presentó una demanda por vulneración del principio de igualdad ante un tribunal de trabajo, debido a que se rechazó en sucesivas ocasiones su candidatura a un ascenso; y, sin embargo, según sostenía, se concedió a colegas con menos méritos, pero todos de sexo masculino.
- Halford tenía derecho a un despacho para su uso exclusivo y en él hacía uso de dos teléfonos, uno de los cuales era para sus comunicaciones privadas y otro de trabajo (estos teléfonos formaban parte de un sistema interno de comunicaciones de la policía, independiente de la red pública).
- La inspectora tuvo conocimiento de que se habían interceptado sus llamadas telefónicas y solicitó a la comisión competente en su país en materia de interceptaciones de comunicaciones, que abriera una investigación puesto que consideraba que tal medida se había realizado para obtener información que sería utilizada contra ella en el curso del procedimiento en materia de discriminación. Como el amparo se le denegó en el país inglés agotadas todas las vías legales en el mismo, acudió al TEDH.

---

la protección contra persecuciones e investigaciones irracionales, y sirvió de base para sentar el criterio de la expectativa razonable de intimidad, conocido también como *expectation of privacy test*. El Tribunal Supremo estadounidense, a lo largo de una extensa y gradual jurisprudencia, ha considerado implícito un «*right to privacy* » en la garantía de la Cuarta Enmienda frente a registros y requisas arbitrarias (*unreasonable searches and seizures*), que limita la intrusión del gobierno en las personas, domicilios, documentos y efectos personales, incluyéndose no sólo los supuestos de invasión material (*physical trespass*) sino también de vigilancia electrónica.

El TEDH consideró que la intercepción de las llamadas de la demandante representaba una violación del art. 8 del CEDH. Para el Tribunal se desprende claramente de su jurisprudencia que las llamadas telefónicas que proceden de locales profesionales, al igual que las procedentes del domicilio, pueden incluirse en los conceptos de «vida privada» y de «correspondencia» citados en el apartado 1 del art. 8 del Convenio de Roma. No hay pruebas de que a la Sra. Halford se le hubiera avisado, en calidad de usuaria de la red interna de telecomunicaciones de la policía, de que las llamadas efectuadas mediante la misma podían ser interceptadas. El Tribunal considera que ella podía razonablemente esperar que se reconociera el carácter privado de este tipo de llamadas.

En el caso *Copland contra el Reino Unido*[16], el TEDH estima que el almacenamiento de la información personal sobre el teléfono de la demandante, su email y el uso que hace de Internet sin su consentimiento suponía una interferencia con su derecho a la vida privada del art. 8 de la CEDH. Durante su empleo en un colegio estatal, el teléfono de la demandante, su email y el uso de internet estuvo sujeto a monitorización por parte de una institución británica ante las sospechas de que la recurrente estaba realizando un abuso de tarificación desde los terminales telefónico e informático. El TEDH declara el quebranto de la expectativa razonable de privacidad, porque la recurrente vivía en un ambiente de permisividad con el que se manejaba en su puesto de trabajo, lo que la había llevado a la creencia de que estaba libre del escrutinio de sus comunicaciones por parte del empleador.

En suma: cuando existe un hábito social generalizado de cierta tolerancia con el uso moderado de los medios informáticos y de comunicación, facilitados por la empresa, se crea una expectativa general de confidencialidad que puede entrar en conflicto con el control empresarial, de ahí la necesidad de regulación mediante convenio colectivo; se

[16] STDH de 3 de abril de 2007 (TEDH 2007, 23).

hace necesario que los representantes de los trabajadores negocien previamente unas reglas de uso que puedan ser asumidas por las partes.

2.2. EL CASO BARBULESCU

La STEDH de 5 de septiembre de 2017[17] conocida como Barbulescu II[18], regula el abanico de protección del derecho

[17] STEDH de 5 de septiembre de 2017 (TEDH 2017, 61).

[18] La Sala Cuarta del STEDH de 12 de enero de 2016, en una primera sentencia conocida como caso Barbulescû *vs.* Romania, avaló el despido de un trabajador de profesión ingeniero, por realizar un uso particular de la cuenta de mensajería de *Yahoo Messenger*, basando su fundamentación en que se demostró que incumplió el código interno de conducta que estaba establecido en la empresa, respecto a la utilización de las tecnologías de la información y de la comunicación. En consecuencia, se podía entender que el empresario podía controlar las comunicaciones electrónicas profesionales de sus empleados, sin vulnerar por ello su derecho a la intimidad, recogido en el art. 8 del CEDH. Los antecedentes del caso son los siguientes: un empleador informó a un trabajador que había realizado un control de la actividad de su cuenta de mensajería instantánea y había comprobado que la había usado para fines particulares, prohibidos por el protocolo sobre uso de nuevas tecnologías establecido en la empresa, por lo cual procedió a su despido disciplinario. En el acto de juicio se aportó como prueba documental de los hechos una transcripción de las comunicaciones de dicha mensajería instantánea, en la que constaban intercambios de mensajes entre el demandado y varias personas e incluso algunos de naturaleza sexual. El demandante negó que *de facto* se cumpliera el protocolo de la empresa, pues, en la práctica había una situación de tolerancia respecto al uso personal de la cuenta profesional de mensajería y alegó que con el registro de esta se había violado su derecho al secreto de la correspondencia. Los tribunales rumanos estimaron la procedencia del despido, por considerar que este se había realizado conforme a la legislación local aplicable, así como la inexistencia de vulneración del derecho a la intimidad del trabajador, por cuanto este había sido informado de la normativa interna de la empresa y el registro de su cuenta de mensajería era la única forma de comprobar si se había respetado esa normativa. El TEDH en una primera Sentencia conocida luego como *Barbulescû I*, concluyó que los tribunales internos mantuvieron un equilibrio apropiado entre el derecho del actor al respeto a su vida privada y a la de su correspondencia electrónica conforme al art. 8 del Convenio y los intereses de su empleador. Por tanto, no se apreció una vulneración de dicho precepto. Si una Sala del TEDH emite una sentencia las partes pueden solicitar la remisión del asunto ante la Gran Sala para una nueva consideración, tal posibilidad es excepcional y de ella hizo uso el demandante, solicitó que el asunto fuera remitido a la Gran Sala; habiendo sido aceptada esta pretensión el 6 de junio de 2016 y procediéndose a dictarse STEDH el 5 de septiembre de 2017, conocida como *Barbulescû II*.

a la autodeterminación informativa, marca doctrina general no sobre mensajería instantánea sino sobre TIC's en general en el marco del contrato del trabajo y de las pautas de control a seguir por el empresario pues construye una técnica argumental de razonamiento genérico para enfrentarse a este tipo de problemas.

El TEDH considera que los tribunales nacionales rumanos han omitido datos fundamentales para resolver el supuesto. Por un lado, verificar si el trabajador había sido advertido con carácter previo por su empresario de la posibilidad de que sus comunicaciones fueran vigiladas, y, por otro lado, la ausencia de información previa y clara ya que, el trabajador no había sido informado ni de la naturaleza, ni del alcance de la vigilancia de la que había sido objeto, así como del grado de intromisión en su vida privada y su correspondencia. Para la mayoría de la Sala, de los hechos declarados probados de la sentencia no puede extraerse la conclusión de que la parte ahora recurrente fuera informada «por anticipado de la extensión y de la naturaleza de la vigilancia llevada a cabo por su empleador», ni tampoco de que este tuviera posibilidad de «acceso al contenido de sus comunicaciones». Lo que conduce a la Gran Sala a considerar que el art. 8 del CEDH es aplicable al supuesto debatido.

El TEDH reflexiona sobre varios aspectos para resolver sobre si se ha vulnerado o no el referido artículo. Surge así una serie de interrogantes que configuran el "test Barbulescu":

- ¿Se ha informado al empleado de la posibilidad de que el empresario tome medidas para controlar su correspondencia y otras comunicaciones, así como de la aplicación de esas medidas? La información debe en principio ser clara en cuanto a la naturaleza de la vigilancia y anterior a su puesta en práctica y en el supuesto enjuiciado no lo ha sido.

El cometido de la Gran Sala, integrada por 15 magistrados, fue revisar la sentencia en base a las excepcionales objeciones alegadas por el recurrente, para reiterar o no el fallo de la misma.

- ¿Cuál fue el alcance de la vigilancia llevada a cabo por el empleador y el grado de intromisión en la vida privada del trabajador? No se detalla, si el empresario hubiera podido valerse de medios menos intrusivos de fiscalización de la cuenta del trabajador, pues se afirma que existen varios tipos de control, unos muy intrusivos sobre el contenido de las comunicaciones electrónicas y otros menos invasores que analizan el tráfico generado sobre el número de las comunicaciones. No se justifica por qué se opta por la vigilancia más intrusiva y no se explica si al mismo resultado se hubiera podido llegar con otros métodos menos invasivos. No se especifica tampoco durante cuánto tiempo se ha llevado a cabo la vigilancia y cuántas personas han podido acceder al contenido de tales informaciones.

- ¿Han existido motivos legítimos, debidamente acreditados por el empleador, para justificar la vigilancia y el acceso a los contenidos de las comunicaciones? Se afirma que no se justifica cuáles son las razones concretas que determinan la fiscalización y monitorización de la cuenta del trabajador, por otro lado, tampoco y, en fin, si el acceso al contenido de las comunicaciones hubiera sido posible sin su conocimiento.

Los tribunales nacionales rumanos no verificaron si el trabajador había sido advertido con anterioridad de la vigilancia que iba a llevarse a cabo de sus comunicaciones electrónicas efectuadas desde la cuenta profesional, ni tampoco hasta qué punto se ha producido una intromisión en la vida privada del trabajador en el ámbito de la relación de trabajo que hubiera podido alcanzarse por vías menos invasivas. Como argumento de cierre, razona la sentencia que no se ha protegido de manera adecuada el derecho del trabajador al respeto de su vida privada, y desde ese momento, no han realizado una ponderación justa de los intereses en juego y han vulnerado el art. 8 CEDH.

2.3. EL CASO LÓPEZ RIBALDA

Con la STEDH de 9 de enero de 2018[19] conocida como *López Ribalda* se reafirma la doctrina anterior *Barbulescu II*, el TEDH estima que la videovigilancia encubierta a las trabajadoras en su puesto de trabajo es una injerencia en su derecho a la vida privada ya que el empresario no cumplió con su obligación de informar a las titulares de los datos de la existencia de la videovigilancia y los fines de la recogida y tratamiento de sus datos personales [20].

El caso López Ribalda y otras contra el Reino de España, resuelve sobre una pretendida vulneración del art. 8 CEDH por lesionar la prueba videográfica el derecho a la privacidad de las cinco demandantes, antiguas empleadas de MERCADONA, en su día despedidas, por haber cometido diversos hurtos.

Los hechos transcurren del siguiente modo: en un supermercado de la cadena antes mencionada, en la provincia de Barcelona, en Granollers, se realizó una auditoría de los últimos meses de facturación que desprendió un importante descuadre contable. Para detectar el origen de las anomalías, se decidió instalar varias cámaras de vigilancia oculta en la línea de caja, para fiscalizar la actividad de los empleados, que a las cámaras permanentes en el área de entrada y de cuya existencia conocían los trabajadores, fiscalizaron la totalidad de la actividad de la plantilla. Del visionado de las grabaciones se constató que varias cajeras cometían pequeños hurtos. Antes de proceder a los correspondientes despidos disciplinarios, las afectadas fueron convocadas a una reunión con presencia de un representante de los trabajadores. En el transcurso de las entrevistas, todas reconocieron los hechos e, incluso, tres de las empleadas firmaron su renuncia a impugnar en sede judicial el despido a cambio de ello, la empleadora ofreció no instar acciones penales contra ellas.

---

[19] STEDH 9 de enero de 2018 (TEDH 2018, 1).

[20] PRECIADO DOMENECH, C.H.: «Comentario de urgencia a la STEDH de 9 de enero de 2018. Caso López Ribalta y otras c. España», *Revista de Información Laboral,* núm. 1, 2018.

Procesalmente se instan dos procesos, en uno de ellos, figuraba como parte accionante una única trabajadora, la señora López Ribalda y, en el otro procedimiento, como parte actora, cuatro trabajadoras. Ambas demandas postulan la nulidad de la prueba por falta de la información previa.

Respecto al art. 8 CEDH, se declara el evidente incumplimiento de su contenido, puesto que el derecho al respeto a la vida privada y familiar, implica un conocimiento previo de la fiscalización de la actividad de las trabajadoras a través de la videovigilancia, y respecto de las cámaras instaladas *ad hoc*, no existía pues no se había facilitado información previa. El Tribunal parte del derecho del empleador a velar por el correcto funcionamiento de su empresa, ejerciendo las correspondientes facultades de control que correspondan, pero siempre salvaguardando un justo equilibrio con los derechos de los trabajadores, lo que en el supuesto objeto de enjuiciamiento no se cumple, argumenta el TEDH.

En la fase de alegaciones, el Reino de España alegó que era cierto que no existía conocimiento de las cámaras ocultas pero que tal omisión no suponía una vulneración del art. 18.4 CE ya que tal medida había superado el juicio de proporcionalidad a través de la regla del triple test. El TEDH discrepa de esta afirmación, entendiendo que no se salvaguardó el correspondiente canon de equilibrio justo entre las partes, lo que provocó una situación de menoscabo hacia los derechos legítimos de las trabajadoras.

Por tanto, el derecho del art. 8 CEDH, ha se ser interpretado de manera abierta, sin prestarse a una definición exhaustiva sino de una *forma dinámicamente amplia* como señala CASAS BAAMONDE[21]. Efectivamente, en la configuración del mencionado derecho existe una doble faceta, negativa y positiva, por un lado, el deber de no injerencia, y por otro

[21] CASAS BAAMONDE, E.: «Informar antes de vigilar, ¿tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral», *Revista de Derecho de Las Relaciones Laborales,* núm. 2, 2018*,* pág. 104.

lado, la obligación positiva de efectividad del derecho tal y como advierte MOLINA NAVARRETE[22].

Por último, con respecto a esta sentencia por parte de la abogacía del Estado representando al Reino de España se ha solicitado que el asunto sea analizado en Gran Sala por los 15 magistrados del TEDH, y tal pretensión ha sido aceptada, por lo que va a dictarse una *López Ribalda II,* que cabe esperar que reafirme la doctrina de la *López Ribalda I*.

3. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

3.1. ÁMBITO DEL RGPD

En un entorno globalizado como el tecnológico, la aplicación extraterritorial de las normas constituye un verdadero desafío, pues no tendría demasiado sentido limitarlas a un determinado espacio, por el principio de aplicación territorial de la Ley, o, a un concreto conjunto de personas, por imperativo del principio de personalidad. Frente al escaso desarrollo que la normativa de protección de datos ha experimentado en el ámbito laboral en nuestro país, a nivel europeo el Reglamento General sobre Protección de Datos (RGPD)[23] abre la posibilidad de intervenir en este ámbito, hasta hace poco ignorado por la normativa estatal.

El RGPD establece una normativa única, válida en toda la UE y aplicable al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado del tratamiento en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

De este modo, el RGPD incorpora nuevas reglas sobre extraterritorialidad de las normas y se aplicará fuera de la Unión Europea cuando el tratamiento de datos personales

[22] MOLINA NAVARRETE, C.: «De "Barbulescu II" a "López Ribalda" ¿qué hay de nuevo en la protección de datos de los trabajadores? Comentario a la Sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2018, caso López Ribalda "et alii" vs. España», *Estudios Financieros, Revista de Trabajo y seguridad social: comentarios casos prácticos: recursos humanos,* núm. 419, 2018*,* pág. 127.

[23] Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y libre circulación de esos datos, DOCE 4 de mayo de 2016.

de interesados residentes en la Unión se efectúe por responsables o encargados del tratamiento no establecidos en la Unión y las actividades de tratamiento estén relacionadas con dos ámbitos:

- La oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se requiere un pago por parte del interesado.
- El control de su conducta, en la medida en que esta tenga lugar en la Unión Europea.

En el ámbito laboral, los aspectos más relevantes del RGPD son los siguientes:

1. El tratamiento de datos está prohibido cuando revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida o la orientación sexual de una persona física[24].
2. El Reglamento da la posibilidad a los Estados miembros de establecer normas más específicas, a través de disposiciones legislativas o de convenios colectivos, para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o

[24] Esta prohibición tiene algunas salvedades en cuanto al tratamiento, *vid*. art. 9.2 del RGPD.

colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

3. Las normas que establezcan los Estados deben incluir medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

4. La figura del *Delegado de Protección de Datos*, ha sido altamente debatida en todo el proceso regulatorio. Existe la obligatoriedad en la designación de dicha figura, pero sólo para determinados casos concretos, como:

- Administraciones Públicas.
- Entidades cuya principal actividad lleve aparejada la monitorización de datos personales o el tratamiento de datos personales a gran escala.

- Entidades cuya principal actividad lleve aparejado el tratamiento de datos especialmente protegidos a gran escala, así como de antecedentes penales.

Con respecto a los derechos de los interesados, existen dos nuevos derechos que son reconocidos a favor de todos los ciudadanos que constituyen una de las principales novedades del RGPD; el derecho al olvido y el derecho a la portabilidad, que a su vez constituyen las dos indicaciones más interesantes que surgen respecto a la aplicación en el ámbito laboral, aspectos, que, por su importancia, se analizan en dos epígrafes separados.

3.2. DERECHO AL OLVIDO

El *derecho al olvido* es una vertiente del derecho a la protección de datos personales frente al uso de la informática y es también un mecanismo de garantía para la preservación de los derechos a la intimidad y al honor, con los que está íntimamente relacionado, aunque se trate de un derecho autónomo [25].

El art. 31.2 RPD establece que en cualquier momento un interesado puede solicitar al responsable de un fichero o tratamiento, que se cancelen los datos que le conciernen, bien porque desee revocar el consentimiento otorgado con anterioridad o bien porque entienda que el tratamiento se está efectuando sin su consentimiento previo o porque no se le ha informado de los extremos que la normativa exige, así el derecho de cancelación dará lugar a la supresión de los datos que resulten inadecuados o excesivos.

Desde que se publicó la conocida STJUE de 13 de mayo de 2014[26] en la que se estimaba la pretensión de un ciudadano español que pedía la cancelación de resultados obtenidos al buscar su nombre en Google, pues mostraba una información desactualizada, se ha ido configurando el «derecho al olvido»[27] y se ha ido concretado su ejercicio. El TJUE reconoció en esta importante sentencia *un cierto derecho a ser olvidados en Internet*[28], derecho del interesado a solicitar que la información sobre su persona no se ponga a disposición del público en general mediante su inclusión en la lista de resultados de los buscadores de Internet, pero no supone un derecho a la supresión de los datos publicados en la Red, es importante resaltar que la sentencia solo se refiere a los buscadores, no comporta el

[25] STC (Sala Pleno), núm. 58/2018 de 4 junio (RTC 2018,58). Constituye la primera sentencia sobre la materia sobre derecho al olvido del TC.

[26] STJUE de 13 mayo 2014 Caso Google Spain S.L contra Agencia Española de Protección de Datos (TJCE 2014, 85).

[27] En el sentido de «desindexación»; alude al derecho de la persona a dejar de tener un perfil *on line*, es decir, a eliminar de la Red su huella digital.

[28] GOÑI SEIN, J. L.: «Los límites de las potestades empresariales *vs.* Derecho de la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral en las redes sociales», *Actum social,* 2015.

derecho a borrar información del soporte original, porque la información personal no se elimina de las webs de origen.
El RGPD fue un poco más allá y configuró, por vez primera, el derecho al olvido como un derecho autónomo a los denominados «derechos ARCO» (acceso, rectificación, cancelación y oposición)[29], en su art. 17. Este derecho plantea dificultades importantes de origen práctico, ya que existen serias restricciones, una de ellas es la imposibilidad de modificar la información contenida en los boletines oficiales, dado que son inalterables una vez transcurrido el plazo para recurrir, otra es la imposibilidad técnica de hacer desaparecer determinadas fotos o noticias una vez que son compartidas en redes sociales, que posteriormente se difunden a otros alojamientos web.
En la práctica, este derecho tiene una dimensión dual: por una parte, para el ciudadano supone un reconocimiento de la pretensión de suprimir de inmediato la información afectada en el sitio web, así como de abstenerse de dar difusión a esta información siempre que el titular de los datos lo solicite. De otra parte, también resulta relevante destacar que este derecho incide en la esfera del responsable del tratamiento, esto es, la entidad, corporación, sitio web o red social que trata los datos. El responsable del tratamiento deberá optar entre limitar el tratamiento del art. 18 RGPD, o bien suprimir sin demora la información, art. 17 RGPD, ponderando caso por caso el alcance de este derecho con el derecho a la libertad de expresión, la salud pública, el deber de conservación de los datos para dar cumplimiento a una obligación legal y el interés público.

3.3. DERECHO A LA PORTABILIDAD DE LOS DATOS

Un segundo límite que no debe desconocerse en el tratamiento de los datos en el ámbito laboral es el *derecho a oponerse a la elaboración de perfiles virtuales*, este derecho no ha tenido unos antecedentes jurisprudenciales tan amplios como los del olvido digital y se ha suscitado

[29] DIAZ DÍAZ, E.: «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones», *Revista Aranzadi Doctrinal*, núm. 6, 2016 (BIB 2016, 3067).

principalmente por razones de interoperabilidad técnica. Se consagra el derecho a la portabilidad en el art. artículo 20 del RGPD Reglamento (UE) 2016/679[30], se debe facilitar la transmisión de datos personales de un proveedor de servicios, como una red social, a otro en un formato estructurado y de uso habitual y de lectura mecánica. Este derecho aumentará la protección en materia de autodeterminación informativa y también mejorará la competencia efectiva entre proveedores de servicios.

Este artículo permite al interesado controlar su disponibilidad *on line*, derecho perfectamente aplicable a los datos subjetivos procedentes de evaluaciones o juicios subjetivos realizados sobre los candidatos a puestos de trabajo o sobre los propios trabajadores, en la práctica el ejercicio del derecho no está exento de complejidades, porque no es nada fácil saber por lo pronto quién posee esos análisis de datos personales (evaluaciones y juicios subjetivos)[31].

---

[30] Dice lo siguiente:

1. *El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y b) el tratamiento se efectúe por medios automatizados.*
2. *Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.*
3. *El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.*
4. *El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.*

[31] GOÑI SEIN, J. L.: «Los límites de las potestades empresariales *vs*. Derecho de la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral en las redes sociales», *op. cit.*

4. LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y GARANTÍA DE DERECHOS DIGITALES

4.1. IDEA GENERAL

La aprobación de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)[32] supone una novedad respecto a la anterior normativa ya que extiende su ámbito material a las relaciones de trabajo. De la propia literalidad del nombre de la Ley y de su Exposición de Motivos, se desvela que son objeto de protección *el derecho a la autodeterminación informativa* (art. 18.4 CE) y los *derechos digitales* que podemos definirlos como derechos y libertades reconocidos a todos los ciudadanos predicables al entorno de Internet[33].

Con tal regulación expresa se ha venido a colmar la laguna existente en la materia[34] y asimismo la DF 13ª de la LO 3/2018 introduce un nuevo artículo 20 *bis* al ET, con el siguiente contenido:

«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».

---

[32] LO 3/2018, de 5 de diciembre. BOE núm. 294, de 6 de diciembre de 2018, páginas 119788 a 119857.

[33] La palabra no se encuentra en la RAE, la definición es transcripción literal de la Exposición de Motivos de la Ley. Por derechos digitales entendemos un elenco heterogéneo de derechos: gran parte de ellos carecen de una relación directa con la protección de datos personales y se conectan más bien con otros derechos fundamentales de las personas, como la igualdad y no discriminación, la libertad de expresión, la intimidad, el honor o la dignidad (neutralidad de Internet, acceso universal a La Red, rectificación en internet o educación digital) y otros derechos digitales, forman parte del núcleo duro del derecho de autodeterminación informativa, como el derecho al olvido, el derecho de portabilidad en servicios de redes sociales y servicios equivalentes o el derecho al testamento digital. *Vid.* GARCÍA MURCIA, J. y RODRÍGUEZ CARDO. I. A.: La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo*, Revista Española de Derecho del Trabajo*, *op. cit*.

[34] Hasta la fecha el terreno era anómico con un único artículo que regulaba de manera manifiestamente insuficiente 20.3 ET.

En definitiva, según el nuevo art. 20 *bis* ET para saber en qué consisten estos derechos de intimidad y desconexión digital, tendremos que acudir a la LOPDGDD, así como a la posibilidad de establecer garantías adicionales a través de la negociación colectiva[35].

En esta regulación de la LOPDGDD tal y como establece en sus artículos 87 a 91 dentro del capítulo X, *Garantía de los Derechos Digitales*[36]*,* se vienen a considerar lícitos los medios de control empresarial a través de las TICs siempre que respeten los derechos constitucionales superando determinados requisitos. El alcance de aplicación en el ámbito laboral es el siguiente:

4.2. USO DE DISPOSITIVOS DIGITALES EN EL ÁMBITO LABORAL

La Ley reconoce expresamente el derecho de los trabajadores a la protección de su intimidad en el uso de los dispositivos digitales puestos a disposición por la empresa. Restringe el acceso del empleador a sus contenidos a los solos efectos de controlar obligaciones laborales o estatutarias y de garantizar la integridad de los dispositivos. Establece el mandato al empleador de fijar los criterios de uso de los dispositivos con la participación de los representantes de los trabajadores, siendo los trabajadores informados de esos criterios.

---

[35] GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo"*, op. cit*.

[36] Dentro del Capítulo X, se entrelazan cuestiones laborales relativas a la intimidad de los trabajadores en el entorno digital, con cuestiones relativas al derecho de acceso a Internet, la seguridad digital, el derecho a la educación digital, el derecho de portabilidad en servicios de redes sociales y equivalentes, o el derecho al testamento digital, materias todas ellas. Pero esta cuestión no es del capítulo, sino que el *totum revolotum* impera en toda la LO existe una mezcla de derechos digitales dentro de una ley dedicada a la protección de datos. El único nexo en común que fuerza el legislador, fijando el herrete en el extremo del cabo para evitar que éste se deshilache es, precisamente, que los derechos y libertades de la Constitución son plenamente aplicables en Internet. *Vid*. QUILEZ QUÑONERO, J.M.: La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores, *Revista Española del Derecho del Trabajo*, núm. 179, 2019.

Como aspecto positivo, hay que destacar la correcta elección del término *dispositivo digital,* cuya amplitud hace referencia a que se entienden incluidos en el mismo tanto los dispositivos digitales actuales en uso (ordenadores, teléfonos móviles, tablets, etc.), como los posibles futuros.
Como primer punto crítico, apuntar que no se recogen de manera expresa los derechos fundamentales del art. 18.3 y del 18.4 CE, como derechos de especial protección dado que también potencialmente junto al 18.1 CE pueden resultar vulnerados. Como segunda objeción, se han dejado fuera de regulación los dispositivos propiedad del trabajador que cada vez se llevan más al trabajo y son usados con fines laborales, de acuerdo con tendencia anglosajona BYOD[37].

4.3. DERECHO A LA DESCONEXIÓN DIGITAL EN EL ÁMBITO LABORAL

La desconexión digital laboral o el derecho a la desconexión laboral es la facultad de los trabajadores a desconectar del trabajo por medios digitales una vez finalizada la jornada laboral convenida[38] .Como precedentes destacables, poner de manifiesto que la figura se encontraba ya regulada en el Derecho francés desde 2016[39]. Es el supuesto de derechos

[37] Siglas de *Bring Your Own Device* (Trae tu propio dispositivo). Con este acrónimo, se describe una nueva tendencia tecnológica en la que la política empresarial permite a los trabajadores utilizar sus propios dispositivos personales para usos profesionales. Asimismo, cuando el empleado además utiliza y comparte aplicaciones y tratamientos poniéndolos a «trabajar» en las funciones de su actividad en la empresa el término se amplía y se habla de BYOT que abarca programas, aplicaciones, plataformas propias o compartidas en el concepto de utilización en común, etc.
En España, muchas empresas por política de ahorro eliminan los móviles corporativos y los sustituyen por subvenciones a los empleados por el uso de su móvil personal para fines profesionales (uso de voz y datos), tendencia que va en aumento, y que se trata de una práctica generalizada en el mundo anglosajón.

[38] PURCALLA BONILLA, M.A.: Control tecnológico de la prestación laboral y derecho a la desconexión de los empleados: Notas a propósito de la Ley 3/2018, de 5 de diciembre, *Revista Española de Derecho del Trabajo*, núm.218, 2019.

[39] Ley número 2016-1088, de 8 de agosto de 2016, relativa al trabajo, la modernización del dialogo social y al aseguramiento de las carreras profesionales (Journal Officiel, núm. 0184, de 9 de agosto de 2016). *Vid*. BARRIOS BAUDOR, G.L.: El derecho a la desconexión digital en el ámbito

digitales más mediático, a pesar de que es una norma abierta, pues remite a la negociación colectiva[40] y en todo caso a la autorregulación del empleador, por ello se ha calificado como un *derecho formalmente novedoso*[41].

Cabe matizar que estamos ante un derecho digital no relacionado con el núcleo duro de autodeterminación informativa. Respecto a la aplicabilidad, se extiende a cualquier forma de trabajo incluido el teletrabajo.

Son varios los factores que motivan la existencia de este derecho por un lado la conciliación de la vida personal y la familiar, por otro lado, la dicotomía entre tiempo de trabajo y de descanso y, finalmente, la prevención del tecnoestrés.

4.4. DISPOSITIVOS DE VIDEOVIGILANCIA Y DE GRABACIÓN DE SONIDOS

El art. 89.1 distingue dos tipos de videovigilancia, la permanente respecto a la que se exige información previa expresa, clara e inequívoca y la encubierta[42] que se permite únicamente en los supuestos de flagrante delito. Los derechos constitucionales que resultan afectados son el

laboral español: primeras aproximaciones, *Revista Aranzadi Doctrinal*, núm. 1, 2019.

[40] Se regula el "derecho a la desconexión digital en el ámbito laboral" (art. 88) para trabajadores y empleados públicos, adaptado a la naturaleza y objeto de la relación y sujeto a lo acordado colectivamente. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna a este respecto. Ya TALENS VISCONTI vaticinó el importante papel de la negociación colectiva en esta materia afirmando que la regulación legal no supondría más que una breve aproximación a un deber empresarial cuyo contenido específico sería aconsejable dejar en manos de la negociación colectiva. Argumentaba que no cabía desconocer que la obligada desconexión digital no afectaba de igual modo ni en la misma intensidad a todas las actividades laborales, por lo que debían de ser los actores legitimados para impulsar la negociación colectiva los que lo dotaran de contenido. *Vid.* TALENS VISCONTI, E.E. La desconexión digital en el ámbito laboral: un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva, *Revista de información Laboral*, núm.4, 2018.

[41] SEMPERE NAVARRO, A. y HIERRO HIERRO, F.J.: Disposiciones Laborales al cierre de 2018, *Aranzadi Digital*, núm. 1, 2019.

[42] En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores se entenderá cumplido el deber de informar cuando existiese al menos el cartel informativo conforme a la instrucción núm.1/2006 de la AEPD.

18.1 CE y 18.4 CE aunque este último no es aludido de manera expresa. El legislador permite el uso de la videovigilancia fundamentando el procesamiento de imágenes en el art. 20.3 ET, como hasta entonces había venido haciendo la jurisprudencia.

Tal distinción entre dos niveles informativos distintos produce posturas encontradas: cierto sector de la doctrina opina que con tal regulación se recoge la jurisprudencia europea[43], otra tendencia considera que al validar la videovigilancia sin información detallada lo que se hace es desoír el mandato del legislador europeo en base a lo preceptuado en el RGPD y en la doctrina López Ribalda y Barbulescu II[44].

El art. 89.2 prohíbe expresamente la instalación de dispositivos de videovigilancia en lugares de descanso o esparcimiento.

---

[43] RODRÍGUEZ ESCANCIANO, S.: Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales, *La Ley*, 15103/2018.

[44] SJS núm. 3 de Pamplona de 18 de febrero de 2019 (AS 2019\1014) El magistrado Carlos González González considera que la inadmisión de la práctica de la prueba videográfica está motivada por la ausencia de información previa, los hechos que motivaron el despido disciplinario en septiembre de 2018 han quedado acreditados por un testigo por lo que se considera el despido procedente. La LOPD entró en vigor después, pero realiza una crítica de la actual regulación que considera incompatible con la regulación comunitaria que ha de primar así la sentencia recoge:

"El art. 89 LOPDRDD plantea muchos interrogantes y el primero de ellos gira en torno a la determinación de los límites inherentes al ejercicio de las funciones de control empresarial y al significado de la expresión "acerca de esta medida" al regular el deber de informar al trabajador ("Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa a los trabajadores o a los empleados públicos y, en su caso, a sus representantes, acerca de esta medida"). Tampoco se concreta si es exigencia legal especifica la finalidad para la que se implantan las medidas de control empresarial y si incluye la finalidad sancionadora en el supuesto de que se graben incumplimientos laborales. Otra omisión sería la relativa al concepto de acto ilícito".

En iguales términos, GONZÁLEZ GONZÁLEZ, C.: Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, *Aranzadi digital*, núm. 1, 2019.

El art. 89.3 regula la posibilidad de la grabación del sonido para supuestos excepcionales únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad.

La norma no determina qué se entiende por tal riesgo, quizás el legislador podía haber concretado especificando qué determinadas actividades son de riesgo, piénsese en determinadas zonas restringidas de una central nuclear, por ejemplo.

Recordemos la doctrina al respecto de la STC 98/2000, de 10 de abril, la grabación del sonido constituye una intromisión *en la propia esfera de desenvolvimiento del individuo*[45] quizás sirva para interpretar el precepto.

- *Art. 90 Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.*

Se establece un deber de información previo a la fiscalización del GPS, que detalle de manera expresa, clara e inequívoca. Se reconocen los derechos de acceso, rectificación, limitación del tratamiento y supresión.

El derecho que resulta más afectado aquí es la autodeterminación informativa (18.4 CE), por su relación instrumental con el derecho a la intimidad este segundo derecho (18.1 CE) también es objeto de protección, pero no de una manera colateral por lo que la redacción del precepto no es del todo afortunada.

- *Art. 91. Derechos digitales de negociación colectiva.*

Dispone que los convenios colectivos podrán establecer garantías adicionales, por lo que la negociación colectiva adquiere un papel relevante para la salvaguarda de estos derechos.

[45] En el caso de las grabaciones del Casino de la Toja, el TC consideró que tal grabación suponía una *intromisión ilegítima en el derecho a la intimidad,* pues la empresa con el sistema de audición y grabación captaba comentarios privados de los clientes y de los trabajadores, que eran ajenos al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales. La actividad que se pretendía controlar por parte de la empresa declaró el TC, se encontraba en lo que ha denominado la *propia esfera de desenvolvimiento del individuo* por lo cual se rebasan las funciones de control en la prestación laboral, que legalmente le concede el ET.

5. EVOLUCIÓN DE LA JURISPRUDENCIA CONSTITUCIONAL

5.1. PRIMERA ETAPA

Durante bastante tiempo, el respeto a la dignidad del trabajador, impuesto por el art. 20.3 ET como límite al ejercicio del control sobre el uso de los medios electrónicos en la empresa, ha quedado confinado a la intimidad y, en algún caso, al secreto de las comunicaciones. La conformidad constitucional de los medios de control se ha examinado solo desde este prisma, relegando a un segundo plano, cuando no obviando, la amalgama de informaciones obtenidas del trabajador consideradas como «*datos personales».* Por tanto, en esta fase, la protección de datos se concibe como una función de garantía del derecho a la intimidad.

5.2. SEGUNDA ETAPA

En la década de los noventa del s. XX empieza a cambiar el planteamiento con la STC 254/1993, de 20 de julio[46], dictada en un recurso donde la protección de datos se concibe como «*un instituto de garantía de otros derechos*», fundamentalmente, «*el honor y la intimidad*», pero también «*un instituto que es en sí mismo un derecho o libertad fundamental».*

El TC procede a estimar el recurso de amparo planteado, por considerar que ha sido vulnerado el derecho del recurrente por la decisión judicial que declaró ajustada a Derecho la denegación presunta del Gobernador Civil de Guipúzcoa y del ministro del Interior de solicitud de información de los datos de carácter personal existentes en ficheros automatizados de la Administración del Estado. De la opinión mayoritaria, disiente un miembro del tribunal, que considera que la pretensión del actor solicitando que se pongan determinados datos personales, no es amparable en virtud del Convenio del Consejo de Europa de 28 de enero de 1981, ratificado por España.

[46] STC 254/1993, de 20 de julio (RTC 1993, 254).

5.3. TERCERA ETAPA

En el inicio del siglo XXI, el proceso de reconocimiento del derecho a la protección de datos como autónomo, marca un precedente importante, con las SSTC 290/2000 y 292/2000. Por un lado, la STC 290/2000, de 30 de noviembre[47], se pronunció sobre la constitucionalidad de la ya entonces derogada Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal de 1992 (LORTAD). Aunque no aborda cuestiones sustantivas sobre el derecho, es muy interesante el voto particular del Magistrado Jiménez de Parga, en el que se expresan las razones por las cuales, a su juicio, *debió afirmarse de modo explícito, en la argumentación de ella, que nuestro Tribunal reconoce y protege ahora un derecho fundamental, el derecho de libertad informática, que no figura en la Tabla del texto de 1978.*

Por su parte la STC 292/2000, de 4 de enero[48], parte del reconocimiento de un derecho fundamental específico, derecho a la protección de datos o libertad informática, que coexiste con otros derechos. Para el Tribunal Constitucional «*la garantía de la vida privada y de la reputación tiene hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad*». Y que se traduce en un derecho de control sobre los datos relativos a la propia persona.

El TC declara la inconstitucionalidad de los incisos «*cuando la comunicación hubiere sido prevista por las disposiciones de creación de fichero o por disposición de superior rango que regule su uso*» del art. 21.1, «*impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas*» y «*o administrativas*» del art. 24.1, y todo el apartado 2 de la LO 15/1999, 13 de diciembre, de Protección de Datos de Carácter Personal.

Entiende la Sala que el límite establecido por el art. 21.1 LOPD, al permitir que una norma de rango inferior a la Ley autorice la cesión de datos entre Administraciones sin previo

[47] STC 290/2000, de 30 de noviembre (RTC 2000, 290).
[48] STC 292/2000, de 30 de noviembre (RTC 2000, 292).

consentimiento del afectado, supone una restricción que sólo podría establecer una Ley, contrariando la reserva legal establecida por el art. 53.1 CE; que la posibilidad de que, con arreglo al art. 24.1 LOPD, la Administración pueda privar al interesado de información relativa al fichero y sus datos, invocando los perjuicios que semejante información pueda acarrear a la persecución de una infracción administrativa, supone una grave restricción de los derechos a la intimidad y a la protección de datos del art. 18.4 CE, y que además «*puede causar grave indefensión al interesado».*

El constituyente quiso garantizar mediante el actual art. 18.4 CE, no solo un ámbito de protección específico sino también más idóneo que el que podrán ofrecer por sí mismos, los derechos fundamentales garantizados en el apartado 1 del precepto.

La peculiaridad de este derecho fundamental a la protección de datos respecto del derecho fundamental a la intimidad radica en su distinta función, lo que apareja por consiguiente que también «*su objeto y contenido difieran*». Insiste después con respecto a este extremo, subrayando que *la función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas, STC 144/1999, de 22 de julio). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado... Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin* (FJ 5.º).

5.4. CUARTA ETAPA

Viene marcada por la STC 29/2013, de 11 de febrero[49], conocida como *caso Universidad de Sevilla*, que constituyó un hito por dos motivos fundamentales; el primero, porque estableció un canon de control de constitucionalidad más rígido que el que la jurisprudencia constitucional venía aplicando respecto al otros derechos fundamentales como el derecho a la intimidad; como segundo motivo, porque por primera vez y únicamente fundamentándose en el art. 18. 4 CE se rechazó el control laboral de la prestación de trabajo. Se denegó la existencia de norma legal en las relaciones laborales que autorizara restricciones del derecho a la información sobre el tratamiento de datos personales, no considerando hábil a tal fin el art. 20. 3 ET. Desde esta máxima, por tanto, negada la validez constitucional de restricciones al derecho fundamental de los trabajadores *ex* art. 18.4 CE, quedaba en consecuencia impedida la ponderación de la medida empresarial, si no había una información a los trabajadores previa y expresa sobre la finalidad de control de la actividad laboral a la que esa captación de imágenes podía ser dirigida.

[49] STC 29/2013, de 11 de febrero (RTC 2013, 29). El Tribunal Constitucional anuló las sanciones impuestas a un subdirector técnico sancionado por una institución universitaria tras ser controlado con respecto al cumplimiento horario con la grabación de las cámaras de videovigilancia que fueron instaladas en los lugares comunes para seguridad de las instalaciones, para conocer si cumplía con su jornada laboral. La Sala consideró lesionado su derecho a la protección de datos. Afirmó que la actuación de la Universidad de Sevilla no podía justificarse por el hecho de que hubiera distintivos para advertir de la instalación de cámaras, sino que era necesario que se informase a los trabajadores de forma previa, precisa y clara de las grabaciones y de su objetivo. En la base de su fundamentación aparece el siguiente relato: *En el caso enjuiciado, las cámaras de videovigilancia instaladas en el recinto universitario reprodujeron la imagen del recurrente y permitieron el control de su jornada de trabajo; captaron, por tanto, su imagen, que constituye un dato de carácter personal, y se emplearon para el seguimiento del cumplimiento de su contrato. De los hechos probados se desprende que la persona jurídica titular del establecimiento donde se encuentran instaladas las videocámaras es la Universidad de Sevilla y que ella fue quien utilizó al fin descrito las grabaciones, siendo la responsable del tratamiento de los datos sin haber informado al trabajador sobre esa utilidad de supervisión laboral asociada a las capturas de su imagen. Vulneró, de esa manera, el art. 18.4 CE* (FJ 8.º).

5.5. QUINTA ETAPA

Está determinada por la STC 39/2016, de 3 de marzo, conocida como *caso Bershka* [50], que modifica muy sustancialmente la doctrina aplicable, se declara que puede haber sistemas sorpresivos o no informados de tratamiento, por lo que la protección del 18.4 CE en esta materia presenta perfiles difusos. Con esta sentencia se reformula la naturaleza de la autorización que recoge la LOPD, que pasa a ser indirecta, y no personal, pese a que estamos ante personas perfectamente individualizables con las que existe una relación contractual.

Se produce, pues, un descenso en el grado de protección del derecho fundamental del art. 18.4 CE, que se añade al dato previo de que la ley ya ha establecido que no es preciso en estos casos el consentimiento, con lo que la información constituía la pieza clave del contenido esencial del mencionado derecho y se entendía cumplido con la existencia de un mero cartel informativo conforme a la Instrucción núm. 1/2006 de la AEPD[51].

[50] STC 39/2016 de 3 marzo (RTC 2016, 39). Versa sobre el despido de una trabajadora de una empresa del grupo INDITEX (Bershka) despidió a una trabajadora por transgresión de la buena fe contractual porque sostenía que se había venido apropiando de efectivo de la caja de la tienda, en diferentes fechas y de forma habitual. Los hechos que dieron lugar al despido fueron conocidos a consecuencia de la instalación de videovigilancia oculta. Para proceder a tal instalación de cámaras ocultas, la empresa argumentó que, a raíz de la instalación de un nuevo sistema de control informático de caja, había detectado que en la tienda y, en concreto, en la caja donde prestaba sus servicios la trabajadora existían múltiples irregularidades, por lo que entendía que había indicios para poder presumir una posible apropiación dineraria por parte de alguno de los trabajadores que operaban en dicha caja. Por tal motivo encargaron a una empresa de seguridad que instalara una cámara de videovigilancia en la tienda donde prestaba sus servicios la demandante y que controlara la mencionada caja en cuestión. La cámara se instaló no habiendo comunicado a los trabajadores dicha instalación, si bien en el escaparate del establecimiento, en un lugar visible, se colocó el distintivo informativo. Se deniega el amparo al validar la prueba de videovigilancia en la que estaba basado.

[51] La Instrucción núm. 1/2006, de 8 de noviembre, de la AEPD sobre tratamiento de datos personales con fines de vigilancia a través de cámaras o videocámaras, especifica que se debe colocar en las zonas videovigiladas al menos un distintivo informativo, ubicado en un lugar suficientemente visible, tanto en espacios abiertos como cerrados,

5.6. SEXTA ETAPA

Con la estela de la STEDH de 5 de septiembre de 2017[52], se vuelve a ampliar el abanico de protección del derecho a la autodeterminación informativa, se marca doctrina general no sobre mensajería instantánea sino sobre TIC's en general en el marco del contrato del trabajo y de las pautas de control a seguir por el empresario pues construye una técnica argumental de razonamiento genérico para enfrentarse a este tipo de problemas.

Con la STEDH de 9 de enero de 2018[53] conocida como *López Ribalda* se reafirma la doctrina anterior del TEDH y con respecto a este particular medio de control se procede a deslegitimar todo tipo de videovigilancia encubierta[54].

Pero la influencia de las dos sentencias[55] va más a allá, implica una modificación a nivel de teoría general destacándose por un sector de la doctrina científica de nuestro país su marcada *vocación generalista,* que no se ciñe*,* obviamente a videovigilancia ni a mensajería instantánea, sino que supone aplicar la protección del derecho a la privacidad a nivel de TICs, ello que supone que se incorpora un plus de protección a los trabajadores, que se logró con la STC 29/2013, pero que se perdió con la STC 39/2016. La doctrina judicial que emana de estas sentencias está llamada a tener importantes consecuencias en la configuración e interpretación de los derechos

asimismo se ha de tener a disposición de los interesados impresos en los que se detalle la información en materia de protección de datos vigente.

[52] STEDH de 5 de septiembre de 2017 (TEDH 2017, 61).

[53] STEDH 9 de enero de 2018 (TEDH 2018, 1).

[54] PRECIADO DOMENECH, C.H.: «Comentario de urgencia a la STEDH de 9 de enero de 2018. Caso López Ribalta y otras c. España», *Revista de Información Laboral,* núm. 1, 2018*.*

[55] La doctrina *López Ribalda*, la siguen: STSJ de Cataluña de 8 enero de 2019 (AS 2019\911) STSJ Madrid 28 septiembre de 2018 (JUR 2018\323429) STJS núm.9 de Sevilla 9 de julio de 2018 (AS 2018\2107) STSJ Cataluña 12 de julio de 2018 (JUR 2018\281030) STSJ Cataluña 25 de junio de 2018 (JUR 2018\227264) STSJ Castilla y León 11 de abril de 2018 (AS 2018\1211)STSJ Castilla-La Mancha 12 de enero de 2018 (AS 2018\566).STSJ País Vasco 27 de febrero de 2018 (AS 2018\1200) y la doctrina *Barbulescu*: STS 8 de febrero de 2018 (RJ 2018\666), STSJ Andalucía de 3 de mayo de 2018 (JUR 2018\210331) y STSJ 28 de marzo de 2019 (ECLI: ES:TSJAND:2019:1355)

fundamentales y en concreto respecto al art. 18.4 CE, ya que supone poder disponer de los datos personales con independencia de su carácter íntimo o no, lo que se concreta jurídicamente en la facultad de acceso a dichos datos, a un ulterior tratamiento, así como su uso o posibles usos por un tercero ya sea el Estado o un particular[56].

Asimismo, dentro de esta doctrina, cabe destacar la STC núm. 25/2019, de 28 de febrero de 2019[57], que aunque no pertenece al ámbito de las relaciones laborales, aplica criterios generales aplicables a todas las jurisdicciones. El precedente de la sentencia cabe situarlo en el arranque en la doctrina de la expectativa en la jurisprudencia constitucional, que tuvo lugar con la publicación de las SSTC 12/2012 de 30 de enero[58] y 74/2012 de 16 de abril[59], referidas ambas a un reportaje periodístico de investigación oculta, rodado en el interior de una clínica sospechosa de intrusismo profesional. Se resolvió el caso concreto dando la razón al titular del derecho a la intimidad, afirmando el TC que, conforme al criterio de expectativa razonable de no ser escuchado u observado por terceras personas, resulta patente que una conversación mantenida en un lugar específicamente ordenado a asegurar la discreción de lo hablado, como ocurre por ejemplo en el despacho donde se realizan las consultas profesionales, pertenece al ámbito de la intimidad.

---

[56] CUADROS GARRIDO, M.E.: «La mensajería instantánea y la STEDH de 5 de septiembre de 2017», *Revista Aranzadi Doctrinal,* núm. 11, 2017.

[57] STC núm.25/2019 de 28 de febrero de 2019 RTC 2019\25

[58] STC 12/2012, de 30 de enero (RTC 2012, 12). Versa sobre un reportaje que la televisión autonómica valenciana emitió, que fue producido por Canal Mundo Producciones, en el que se utilizaban imágenes obtenidas mediante cámara oculta. El canal de televisión y la productora fueron condenados por intromisión a la intimidad y vulneración del derecho a la propia imagen. La sentencia recoge la jurisprudencia del Tribunal Europeo de Derechos Humanos, haciéndose eco de la teoría de la expectativa razonable. De este modo, concluye que la conversación mantenida en un lugar específicamente ordenado a asegurar la discrecionalidad de lo hablado –en este caso concreto una consulta profesional– pertenece al ámbito de la intimidad. En consecuencia, se desestima el recurso de amparo interpuesto.

[59] STC 74/2012, de 16 de abril (RTC 2012, 74).

El supuesto enjuiciado en la STC núm. 25/2019, de 28 de febrero de 2019, es muy similar al anterior, se trata de un reportaje periodístico sobre un pretendido sanador que como parte de lo que ofertaba daba la posibilidad de dar una copia en DVD de los servicios prestados, pero, además, los periodistas infiltrados como supuestos clientes utilizaron cámaras ocultas[60]. El TS estima en parte el recurso y casa la STS pues considera que con respecto a la grabación de las imágenes encubiertas se lesionó el derecho del recurrente a la intimidad personal, la propia imagen y el honor al centrarse los programas televisivos en la persona del demandante de amparo y difundir un material insuficientemente concluyente de por sí y escasamente relevante para contribuir a un debate general. Por lo que la intromisión en su intimidad, no solo careció del, en principio, necesario consentimiento previo del titular del derecho para realizar la videograbación en la consulta profesional, sino que, en las circunstancias del caso, su divulgación constituyó también un ejercicio desproporcionado de la libertad de información.

[60] El 3 de diciembre de 2010, dos periodistas acudieron un despacho de una persona que ejercía como coach , mentor y consultor personal, haciéndose pasar por clientes y fingiendo uno de ellos que padecía cáncer, y grabaron la visita con cámara oculta. Al día siguiente los periodistas regresaron al mismo despacho para recoger la grabación de la visita ya que el curador grababa a su vez todas las visitas y proporcionaba una copia a sus clientes: los periodistas también grabaron esa nueva visita con cámara oculta. El día 15 de diciembre de 2010 se emitieron fragmentos de las grabaciones de las visitas obtenidas con cámara oculta en el programa «Espejo Público» de la entidad mercantil Antena 3 de Televisión, S.A. En el programa los antes citados periodistas debatieron con la conductora del programa y otros colaboradores sobre las visitas realizadas y sobre la actuación y el modo de proceder del demandante de amparo. El debate se centró en mostrarle como un "sanador" que no teniendo titulación alguna relacionada con la salud se atribuía aptitud para curar todo tipo de enfermedades; asimismo, se le calificó de "mujeriego" y se le imputó incluir en las terapias "algo más que caricias". Asimismo, en el programa «3 D» de la misma entidad Antena 3 se emitió un reportaje titulado "¿Un falso gurú de la felicidad?" sobre el demandante de amparo en el que se mezclaban videos grabados por él mismo con entrevistas y material propio de la cadena. También se reprodujeron fragmentos del reportaje en otros programas de noticias de Antena 3 y en la página web de la misma cadena televisiva bajo el titular "El presunto sanador de Mallorca, al descubierto. Acudimos a su consulta en Mallorca".

El TC afirma que no puede obviarse la circunstancia de que la información fuera captada subrepticiamente en un ámbito privado como es una consulta profesional, en cuyo seno se desarrollan relaciones de naturaleza profesional que están también protegidas por el derecho a la intimidad, y en las que, por consiguiente, existe igualmente una legítima expectativa de resguardo frente a la intromisión de terceros.

Por otro lado, considera el TC que el hecho de que el recurrente proporcionara una grabación de la misma sesión que los periodistas filmaron con cámara oculta, no subsana en absoluto la ausencia de consentimiento para realizar la grabación subrepticia y divulgar las imágenes así obtenidas, ni implica un consentimiento expreso, válido y eficaz para difundir públicamente en un medio de comunicación social las imágenes contenidas en la grabación proporcionada; por el contrario, pone de manifiesto que la grabación oculta que llevaron a cabo los periodistas, así como su posterior difusión, no fue necesaria para obtener la información y difundirla.

De este modo, el TC hace propia la esencia misma del concepto de *expectativa razonable de privacidad*; reside en derivar los contornos mismos del derecho fundamental concernido del entorno de la privacidad, no tanto en su configuración formal, como en ese poder que todo ciudadano tiene de hacerlo valer, frente a los poderes públicos o al resto de la sociedad, el llamado *derecho de exclusión*.

Por último, dentro de esta etapa cabe mencionar la reciente STS de 10 de abril de 2019[61]. Los hechos enjuiciados en ella son los siguientes: una empresa multinacional de telemarketing que realiza servicios de *contact center,* incluye en una de las cláusulas del contrato de trabajo[62] la

[61] STS de 10 de abril de 2019 (ECLI: ES:TS:2019:1436).

[62] "El trabajador consiente expresamente, conforme a la LO 1/1982, de 5 de mayo, RD 1720/2007 de Protección de Datos de carácter personal y Ley Orgánica 3/1985 de 29 de mayo, a la cesión de su imagen, tomada mediante cámara web o cualquier otro medio, siempre con el fin de desarrollar una actividad propia de telemarketing y cumplir, por tanto, con el objeto del presente contrato y los requerimientos del contrato mercantil del cliente".

autorización expresa para grabar mediante la cámara web o dispositivo análogo la imagen del trabajador con el fin del correcto desarrollo de la prestación laboral. Tal uso de la imagen no era habitual sino puntual, reservado para determinadas actividades promocionales, en las que se solicitaba una autorización específica a los trabajadores. Con la introducción de la cláusula genérica se pretendía eludir la petición de autorizaciones *ad hoc* cada vez que fuera necesario.

El sindicato CGT presente en la empresa impugna la referida cláusula ante la Audiencia Nacional planteando un conflicto colectivo, a la demanda se adhieren el resto de los sindicatos con representación en la empresa. La AN estima la demanda y declara la nulidad de la cláusula de cesión de la imagen por no ser válida por violar el derecho a la propia imagen del empleado. No conforme con el fallo, la empresa recurre la decisión al TS en casación y el recurso es estimado y, por tanto, la sentencia de la Audiencia anulada. El TS entiende que la restricción del derecho es viable cuando el objeto del contrato lo sobrentiende, como ocurre en el presente caso, dado que la ejecución es la realización de labores de telemarketing incluso con videollamadas. Por lo que esta mayor intrusión se tolera por el especial objeto del contrato de trabajo, y dadas las especiales características, a diferencia de un contrato de trabajo ordinario.

El debate jurídico que plantea la STS de 10 de abril de 2019 nos lleva a partir de que el telemarketing lleva implícito que se graben las conversaciones. Desde el punto de vista del trabajador, la grabación de la conversación puede ser mucho más sensible, que otro tipo de seguimientos por parte del empresario, suponer una mayor invasión de la intimidad que una imagen, porque puede relevar pensamientos o sentimientos internos que el otro medio no proporciona, en este sentido el art 89.3 de la LOPDGDD. El hecho cierto es que, si las conversaciones no pudieran ser grabadas, y en su caso controladas, la prestación tampoco podría ser dirigida y vigilada por el empresario, por lo que el control de las conversaciones es indispensable por la propia lógica del contrato, se ha de realizar en unas condiciones

que minimicen la eventual lesión de la esfera de la intimidad, a través de los ya controles aleatorios. La STS de 5 de diciembre de 2003[63] marcó un hito en esta materia y de su doctrina hemos de partir para interpretar el supuesto comentado. El TS considera que el derecho a la propia imagen al que se refiere la AN se encuentra tutelado en el art. 18.4 CE, dado que la imagen es un dato personal, en base a ello, dada la redacción de la anterior LOPD y el RGD[64], no es necesario recabar el consentimiento del trabajador, puesto que se trata de una de las exclusiones que marcan ambos textos legislativos. El hecho de grabar la imagen es algo puntual, cuando las exigencias de las actividades promocionales lo requieran, pero en todo caso forma parte del propio contrato de trabajo, por lo que cabe concluir que la cláusula controvertida no es abusiva, sino, más bien, informativa y a la par receptora de un consentimiento expreso que no era preciso requerir.

A continuación, para dar más fuerza al argumento se trae a colación la doctrina de la STC 99/1994, de 11 de abril[65], que considera aplicable, se ha respetado, en el caso enjuiciado

[63] STS de 5 de diciembre de 2003 (RJ 2004, 313). En ella el Tribunal Supremo no encontró ningún inconveniente para no permitir al empleador intervenir el contenido de las conversaciones telefónicas mantenidas por los trabajadores cuando existía una finalidad legítima que justificara la intromisión, como lo era, en un supuesto de telemarketing, analizar las técnicas comerciales de los trabajadores para impartir las oportunas instrucciones para mejorarlas. Se desestimó que existiera una lesión del derecho a la intimidad, por la grabación de conversaciones entre los trabajadores (asesores comerciales de Telefónica) y sus clientes, aplicando el principio de ponderación, pues la medida es idónea para la finalidad pretendida, necesaria y equilibrada.

[64] Respecto al RGPD el TS precisa que *la nueva normativa coincide con la anterior y, aunque rigoriza ciertas cuestiones, flexibiliza y hace más clara la aplicación de otros principios como el del consentimiento del interesado, que no es preciso que se preste expresamente cuando el tratamiento del dato es necesario para la ejecución de un contrato suscrito por el interesado, artículos 6-1-b) y 9-2-b) del Reglamento Comunitario*.

[65] STC 99/1994, de 11 de abril (RTC 1994, 99). Conocida como el caso del *cortador de jamón*, estimó lesivo el derecho al uso de la propia imagen del trabajador que fue despedido por su negativa a obedecer la orden empresarial que le obligaba a exhibir en público su habilidad profesional como deshuesador de jamones en un acto promocional con presencia de los medios de comunicación.

el principio de indispensabilidad o de estricta necesidad de la limitación, en base al cual el equilibrio entre las obligaciones derivadas del contrato para el trabajador y el ámbito de su libertad constitucional ha de producirse en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva.
Por último, el TS precisa que no se está ante un supuesto de videovigilancia, sino ante *videollamadas* en las que quien llama, gracias a una cámara webcam que instala la empresa, ve a quien le atiende y conversa con su interlocutor. Ese es el dato que se le cede y facilita, pero que luego no puede tratar haciendo una grabación y otras operaciones, pues ello está expresamente prohibido de manera genérica como principio general en el art 5-1-b RGD.

6. REFLEXIONES CONCLUSIVAS

PRIMERA. Es conveniente establecer una política empresarial admonitiva y preventiva sobre el uso de los dispositivos digitales puestos a disposición de la empresa, teniendo en cuenta lo siguiente:

- Antes del inicio de la relación laboral, se han de establecer previamente las reglas del juego; se ha de informar de manera clara suficiente al trabajador de la política de la empresa respecto al uso de las nuevas tecnologías y su posible uso disciplinario.

- Una vez iniciada la relación laboral, se ha de usar la tecnología informática de manera preventiva, para evitar "fugas de información".

-No son aconsejables las prohibiciones absolutas, sino un uso de las TICS social moderado.

- Durante el transcurso de la relación laboral, se han de realizar de manera esporádica controles aleatorios para no convertir en tolerancia ciertas prácticas o malos hábitos que pudieran existir (si se prohíbe, pero no se controla se puede crear un clima de permisividad).

SEGUNDA. El derecho del art 18.4 CE se encuentra en construcción puesto que sus límites son difusos y no están aún determinados.

TERCERA. La regulación por parte de la LOPDGDD en materia laboral con los arts. 97 a 91, supone un gran avance significativo, pero no ha respondido a las expectativas. El papel de la negociación colectiva en esta materia adquiere el rol de protagonista, en una tarea que cabe vaticinar que no va a ser fácil.

CUARTA. A nivel general en materia de protección de datos, la ley insta a confusión, en ocasiones, pues parece que entiende que la intimidad equivale a autodeterminación informativa. Y tampoco distingue de una manera clara entre derechos digitales y protección de datos, pues a veces trata los términos como sinónimos.

7. BIBLIOGRAFÍA

BARRIOS BAUDOR, G.L: «El derecho a la desconexión digital en el ámbito laboral español: primeras aproximaciones», *Revista Aranzadi Doctrinal*, núm. 1, 2019.

CASAS BAAMONDE, M.E.: «Informar antes de vigilar, ¿tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral», *Revista de Derecho de Las Relaciones Laborales,* núm. 2, 2018.

CÓRDOBA CASTROVERDE, D. y DÍEZ-PICAZO GIMENÉZ, L. M.: «Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico», XX Jornadas de la Asociación de Letrados del Tribunal Constitucional/coord. por Asociación de Letrados del Tribunal Constitucional (España), 2016.

CUADROS GARRIDO, M.E.:

-*Trabajadores Tecnológicos y Empresas Digitales*, Aranzadi, 2018.

-«La mensajería instantánea y la STEDH de 5 de septiembre de 2017», *Revista Aranzadi Doctrinal,* núm. 11, 2017.

DÍAZ DÍAZ, E.: «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones», *Revista Aranzadi Doctrinal*, núm. 6, 2016.

GARCÍA MURCIA, J. y RODRÍGUEZ CARDO. I.A.: «La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo»*, Revista Española de Derecho del Trabajo*, núm. 216, 2019.

GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, J. R: «La protección de datos se come a la intimidad: la doctrina de la sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (caso Bărbulescu v. Rumania; nº 61496/08; Gran Sala), *Revista de Información Laboral*, núm. 10, 2017.

GONZÁLEZ GONZÁLEZ, C.: «Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales», *Aranzadi digital*, núm. 1, 2019.

GOÑI SEIN, J.L.: «Los límites de las potestades empresariales *vs.* Derecho de la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral en las redes sociales», *Actum social,* 2015.

MOLINA NAVARRETE, C.: «De "Barbulescu II" a "López Ribalda" ¿qué hay de nuevo en la protección de datos de los trabajadores? Comentario a la Sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2018, caso López Ribalda "et alii" vs. España», *Estudios Financieros, Revista de Trabajo y seguridad social: comentarios casos prácticos: recursos humanos,* núm. 419, 2018.

PRECIADO DOMENECH, C.H.: «Comentario de urgencia a la STEDH de 9 de enero de 2018. Caso López Ribalta y otras c. España», *Revista de Información Laboral,* núm. 1, 2018.

PURCALLA BONILLA, M. A.: «Control tecnológico de la prestación laboral y derecho a la desconexión de los empleados: Notas a propósito de la Ley 3/2018, de 5 de diciembre», *Revista Española de Derecho del Trabajo*, núm.218, 2019.

RODRÍGUEZ ESCANCIANO, S.: «Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales», *La Ley*, 15103/2018.

SEMPERE NAVARRO, A.V. y HIERRO HIERRO, F.J.: «Disposiciones Laborales al cierre de 2018», *Aranzadi Digital*, núm. 1, 2019.

SEMPERE NAVARRO, A. V. y SAN MARTÍN MAZZUCCONI, C.: «*Nuevas tecnologías y Relaciones Laborales*», Aranzadi, 2002.

TALENS VISCONTI, E.E. «La desconexión digital en el ámbito laboral: un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva», *Revista de información Laboral*, núm. 4, 2018.