ACCESO A DISPOSITIVOS DIGITALES DEL TRABAJADOR FACILITADOS POR LA EMPRESA

Dr. Manuel Luque Parra[1] y Dr. Francisco Ramón Lacomba[2]

Sumario

Abstract: El presente capítulo aborda el análisis de la compleja delimitación legal y jurisprudencial de los límites a la facultad empresarial de registro de sus dispositivos digitales facilitados a sus trabajadores para la ejecución de su prestación laboral. El potencial uso privado por los trabajadores de estos dispositivos, incluso aunque se prohíba por la empresa, plantea el riesgo de vulneración de los derechos de intimidad, secreto de las comunicaciones y protección de datos de carácter personal del trabajador, cuya salvaguarda debe encontrar el adecuado equilibrio con la protección del legítimo derecho del empleador derivado de la libertad de empresa también constitucionalmente protegida.

Palabras clave: registro, ordenadores, dispositivos digitales, intimidad, secreto de las comunicaciones, protección de datos, derechos digitales, monitorización prueba lícita, doctrina de los frutos del árbol envenenado, Bărbulescu, López Ribalda, desconexión digital

[1] Catedrático de Derecho del Trabajo y la Seguridad Social de la Universidad Pompeu Fabra. Consejero académico de Cuatrecasas.
[2] Abogado laboralista del Área de Conocimiento e Innovación de Cuatrecasas. Profesor asociado de la Universidad de Valencia

1. INTRODUCCIÓN

El reconocimiento constitucional del principio de libertad de empresa constituye el fundamento básico de los poderes de dirección y organización atribuidos al empresario, que incluyen, entre otras, la facultad de controlar que el trabajador cumple con su contrato de trabajo.

El punto de partida normativo para establecer el alcance de tal facultad de control empresarial se sitúa originariamente en el art. 20.3 ET, que fija sus límites generales en los siguientes términos: *"el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales,* ***guardando en su adopción y aplicación la consideración debida a su dignidad*** *y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad"*[3]. El texto del indicado precepto está cerca de cumplir los 40 años de edad, puesto que ha permanecido prácticamente inalterado hasta la actualidad desde su redacción original en la Ley 8/1980, de 10 de marzo, del Estatuto de los Trabajadores.

Las realidades empresarial y sociolaboral, sin embargo, han cambiado mucho desde entonces. Es un hecho que, en cada vez más puestos de trabajo, se ha flexibilizado la nota de dependencia, esto es, el asalariado es más autónomo en el desarrollo de sus funciones, que realiza en buena parte al margen de cualquier supervisión directa; también se ha desdibujado el aspecto locativo de la prestación laboral, pasando cada vez más trabajadores de encontrarse en un lugar de trabajo bajo la directa fiscalización del empleador a desempeñar sus funciones desplazados, teletrabajando[4], etc, es decir, alejados de la mirada del empresario; y es también un dato clave que la digitalización de la información de la empresa (de sus secretos también) ha facilitado el riesgo de su extracción por los trabajadores. Todo ello ha alimentado cierta ansiedad empresarial de ejercer una mayor vigilancia o comprobación de la prestación laboral, tanto preventivamente como *a posteriori*, ante cualquier hecho sospechoso.

En la actualidad, además, ese control sobre el trabajador puede ser más intenso y eficaz gracias a dos factores tecnológicos facilitadores:

- Por un lado, el hecho creciente de que gran parte de la actividad del trabajador deje rastro o sea visible a través de los dispositivos digitales corporativos (ordenadores, tablets, móviles…), con acceso a la red (interna o externa), que la propia empresa le facilita para el cumplimiento de sus funciones, merced a la imparable transformación digital de las organizaciones.

- Por otro lado, la evidencia de que la evolución de la tecnología permite hoy con más facilidad el seguimiento en directo y la grabación de la actividad del trabajador, sus imágenes o audio o su geolocalización.

[3] El propio ET establece normas específicas en relación con el poder empresarial de control del trabajo. Así el art. 18 ET regula los registros sobre la persona del trabajador, sus efectos personales y taquillas en defensa del patrimonio empresarial y de otros trabajadores; y el art. 20.4 ET se ocupa del control por la empresa de la enfermedad del trabajador que justificaría su falta de asistencia al trabajo.

[4] LUQUE PARRA, M. y GINÈS I FABRELLAS, A. *Teletrabajo y prevención de riesgos laborales*, CEOE-Fundación para la Prevención de Riesgos Laborales. Madrid, 2016. ISBN 978-84-608-3498-4. Pp. 1 a 119.

Todo ello ha generado un considerable incremento de los conflictos derivados del ejercicio cada vez mayor por la empresa de sus poderes de control, a través del acceso a los ordenadores y otros dispositivos digitales que utilizan los trabajadores para el desempeño de sus funciones. En tales litigios, la discusión se centra principalmente en si la información así recabada, que ha servido a la empresa como medio de prueba (a veces, único) de la supuesta infracción laboral cometida por el trabajador, se ha obtenido lícitamente a los efectos de otorgarle eficacia probatoria o negársela e, incluso, contaminar de nulidad la medida disciplinaria.

Este nuevo escenario tecnológico ha puesto de manifiesto la necesidad gradual de ir construyendo una respuesta más elaborada tanto desde el ámbito normativo como judicial en torno a los límites oponibles a la facultad empresarial de control y vigilancia en relación con estos dispositivos, habida cuenta de su potencial uso privado por los trabajadores y, por tanto, de que se vean expuestos sus derechos de intimidad, secreto de las comunicaciones y protección de datos de carácter personal que reconoce el art. 18 CE.

No es exagerado afirmar que nos encontramos en un momento histórico en el que, ante la nueva realidad digital de las empresas, el legislador y los tribunales están precisando los límites a la actuación empresarial que, en relación con la posible vulneración de derechos fundamentales, deberá observar el ejercicio de la facultad de control empresarial en estos casos cada vez más habituales.

Dos hitos principales, entre otros, marcan los últimos puntos de inflexión en esta materia tan presente ya en la rutina laboral de tantas personas:

- De una parte, la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), que introduce un reconocimiento expreso del derecho de los trabajadores a la protección de su intimidad en el uso de los dispositivos digitales de la empresa, a través del nuevo art. 20.bis ET y de su art. 87. Aunque, a la vez, la norma permite a la empresa acceder a tales dispositivos a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de los mismos, imponiendo, eso sí, dar seguridad a los trabajadores acerca sus expectativas de intimidad en el uso de estos dispositivos, mediante el establecimiento previo (con participación de los representantes de los trabajadores) de los criterios de utilización de estos medios de trabajo y la concreción de los posibles usos privados, de todo lo que deberá informarse a los trabajadores.

- De otra parte, es de obligada referencia la Sentencia de la Gran Sala del Tribunal Europeo de Derecho Humanos (STEDH) de 05-09-2017 (asunto Bărbulescu-II), que revocó el criterio de la anterior STEDH 12-01-2016 (Bărbulescu-I) y que, entre otras referencias, ha considerado que *«es una vulneración del derecho a la intimidad y al secreto de las comunicaciones vigilar los mensajes enviados por un trabajador mediante medios propios de la empresa y acceder al contenido de los mismos, si no ha sido previamente informado de esta posibilidad, incluso si existían normas en la empresa que prohíban su utilización con fines personales»*.

La configuración de los límites a esta facultad empresarial de registro de dispositivos digitales puestos a disposición de los trabajadores sigue hoy, pese a todo, en revisión y construyéndose con cada nuevo conflicto que llega a los Tribunales, cuya actuación en orden a ir precisando tales parámetros de licitud capitaliza la actualidad en esta materia.

Pero, no está siendo una construcción fácil. La nueva regulación legal puede suscitar algunas dudas y, sobre todo, los Tribunales no han cerrado totalmente aún una posición firme al respecto, como lo prueba que el TEDH haya cambiado internamente su parecer, en breve tiempo, en dos asuntos tan importantes para estas materias como Bărbulescu o López Ribalda[5], en los que la Gran Sala ha revocado en pocos meses el criterio de la anterior sentencia del Tribunal.

En juego se encuentra tanto el interés empresarial en la defensa de su patrimonio frente a incumplimientos contractuales de un trabajador cada vez más esquivos, solo detectables por la vía del registro de dispositivos digitales, como el interés del trabajador en que ese registro no haya invadido su esfera de privacidad. Ambos necesitan seguridad jurídica en esta materia y, en nuestro caso, corresponde a los Tribunales españoles hacer suya la doctrina judicial europea e integrarla coherentemente en nuestra propia doctrina judicial.

En este sentido, sin embargo, nos preocupan los sutiles puntos de disonancia existentes en algunos aspectos de la posición de nuestros Tribunales. En concreto, puntos clave a efectos del registro de dispositivos digitales como la cobertura que dispensa a la empresa disponer de un código de conducta de "tolerancia cero", esto es, que prohíba cualquier uso privado, o la suficiencia para la empresa de actuar en esos registros conforme a las reglas de uso establecidas, sin considerar la idoneidad, proporcionalidad, necesidad y razonabilidad de la medida, no se están valorando del mismo modo por la doctrina europea y por los Tribunales españoles.

Para el análisis de estas y otras cuestiones de interés en relación con la facultad de control empresarial sobre dispositivos digitales, seguiremos la siguiente secuencia. En primer lugar, empezaremos por entender el contexto en el que se produce el ejercicio de esta facultad. A continuación, será parada obligada la dimensión constitucional que alcanza este poder empresarial de control, a los efectos de traer a colación el juego de los límites derivados de la afectación a derechos fundamentales del trabajador. El paso siguiente habrá de ser descender a la legalidad vigente para concretar qué parámetros legales de licitud se han impuesto al ejercicio, en estos supuestos, de la facultad empresarial de control. Y, por último, deberemos situarnos en la doctrina judicial, a los efectos también de detectar la recepción por nuestros órganos jurisdiccionales de la doctrina judicial europea.

Vamos a optar, además, por un formato ágil de pregunta-respuesta, que nos ha de permitir avanzar hacia la reconstrucción de los criterios legales y judiciales esenciales en relación con la actuación empresarial en esta materia.

En definitiva, con todo ello, trataremos de precisar las reglas de juego básicas que, gradualmente, la intervención del legislador y de los Tribunales están contribuyendo a precisar, a fin de que empresas y trabajadores despejen sus dudas acerca de los límites al registro de ordenadores y otros dispositivos digitales.

2. CONTEXTUALIZACIÓN

Frente a la sospechada o potencial infracción laboral del trabajador, es legítimo que la empresa reaccione y trate de asegurarse la viabilidad de su respuesta sancionadora. Tal y como sucede ante cualquier posible incumplimiento del trabajador, la estrategia empresarial consistirá en

[5] STEDH, Gran Sala, 17-10-2019 (Asuntos 1874/13 y 8567/13)

detectar y confirmar los hechos y reunir medios de prueba para que, si se requiere, pueda aportarlos en el futuro.

Pero, cuando esos hechos constitutivos de infracción, o una parte de ellos, se constatan a través del registro de dispositivos digitales puestos a disposición del trabajador, la viabilidad del esfuerzo probatorio se complica debido a la posible vulneración de derechos fundamentales del trabajador implicados en el uso privado de tales dispositivos.

Este es, pues, el contexto del debate en torno a la facultad de control empresarial en esta materia, que queda comprendido entre las siguientes coordenadas:

- La singularidad del objeto del registro, que comprende dispositivos y recursos digitales donde, como veremos, se ponen en juego derechos fundamentales del trabajador.

- La gravedad del objetivo del registro, que puede culminar en el ejercicio del poder disciplinario de la empresa, que también es legítimo y merecedor, por tanto, de su espacio de protección.

- Su ineludible transcendencia procesal, puesto que, es en sede judicial donde se juega verdaderamente su éxito el registro empresarial de los ordenadores y otros dispositivos digitales, no solo como medio de prueba, sino hasta el punto de que puede acarrear la nulidad la medida disciplinaria, merced a la llamada «doctrina de los frutos del árbol envenenado».

Las siguientes preguntas, y sus respuestas, en relación con cada uno de estos puntos, nos deberían ayudar a situar la frontera del ejercicio problemático de la facultad de control empresarial en este ámbito.

a) Delimitación del objeto del registro

2.1 Cuando hablamos de registro del ordenador, ¿hablamos solo del registro del e-mail?

No únicamente. En realidad, nos estamos refiriendo al registro del contenido de cualquier dispositivo electrónico que la empresa ponga a disposición del trabajador, con cualquier aplicación instalada o funcionalidad habilitada susceptible de dejar en dicho dispositivo algún rastro accesible de su uso privado.

2.2 Entonces, ¿la facultad de registro y control por la empresa se ha de sujetar a los mismos límites cuando se trate de smartphones o iphones, una tablet, un USB o cualquier otro recurso electrónico o telemático que facilite la empresa?

Sí, en la medida en que los mismos operen como instrumentos hábiles para enviar o recibir e-mails o mensajes personales, y/o para almacenar información privada, ya que se convierten en soportes físicos donde puede quedar afectado el derecho a la intimidad personal, al quedar todos esos datos disponibles en la memoria del terminal informático o digital utilizado de que se trate.

2.3 Qué sucede con los emails que envía el trabajador desde la dirección profesional, pero accediendo desde su ordenador personal

El riesgo para los derechos fundamentales del trabajador es el mismo. El control, en este caso, se efectuaría a través de la copia en el servidor de la empresa, por lo que la situación no diferiría del registro físico del ordenador profesional utilizado directamente por el trabajador.

b) Delimitación del objetivo del registro

2.4 ¿Cuáles son las finalidades legítimas del control y registro de dispositivos digitales que activarían el riesgo sobre los derechos fundamentales del trabajador?

Las finalidades habituales del registro desde el punto de vista empresarial pueden ser dos:

- Preventiva, es decir, comprobar rutinariamente si el trabajador está desarrollando correctamente su actividad laboral. En estos casos, atendiendo al alcance subjetivo amplio y no temporal de la monitorización, el test de proporcionalidad constitucional al que nos referiremos más adelante debería ser más tuitivo con los derechos de los trabajadores.

- Reactiva, esto es, que la empresa haya detectado un incumplimiento (o sospeche que se ha producido) verificable a través del ordenador o dispositivo digital del trabajador y aquélla haya de procedimentalizar esa sanción. Aquí es, fundamentalmente, suele surgir la duda sobre si el registro podía realizarse y con qué alcance.

2.5 ¿Cuál podría ser un ejemplo de registro de ordenadores con finalidad preventiva?

Ilustra sobre dicho control preventivo el asunto que aborda, por ejemplo, la STSJ C. Valenciana (Social) núm. 2716/2010, de 5 octubre (Rec. 2195/2010), en el que la empresa entregó a todo el personal una notificación con la que se informaba que a partir de esa fecha *«la empresa dispone de un programa para contabilizar el tiempo que cada trabajador emplea en Internet, así como el registro de las direcciones que visita, de la misma forma que realizará con el correo electrónico. Se recuerda que tanto Internet como el correo electrónico son herramientas que la empresa pone a disposición del trabajador para poder desarrollar sus tareas de una forma más rápida y eficaz. Todo uso inadecuado de ambas herramientas será registrado y grabado»*.

Como consecuencia de ese seguimiento rutinario, la empresa descubre la infracción laboral del trabajador y procede a su sanción.

2.6 ¿Cuál podría ser un ejemplo de registro de ordenadores con finalidad reactiva?

Recoge un supuesto de registro reactivo del ordenador del trabajador, por ejemplo, la Sentencia de Juzgado de lo Social núm. 2 de Palma de Mallorca, núm. 291/2019, de 30 de agosto de 2019 (autos 1014/2017). En la misma, se juzga un supuesto en el que *«la investigación del ordenador se llevó a cabo como consecuencia de una sospecha fundada, basada tanto en la queja directa del compañero que trabajaba en el mismo departamento que la actora, quien manifestó a la coordinadora el incumplimiento de las tareas que la* (actora) *tenía encomendadas y el incremento que había supuesto para él en su volumen de trabajo, como en las propias comprobaciones rutinarias que la coordinadora llevaba a cabo en las que pudo observar un elevado volumen de accesos a internet realizados por la demandante que le llamó la atención, tal y como declaró en el acto de la vista»*.

2.7 ¿Existe alguna finalidad preventiva del registro de ordenadores que la empresa pueda verse obligada a atender por exigencia legal?

Sí. El art. 88 LOPDGDD reconoce a los trabajadores y empleados públicos *"el derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar"*. De esta manera, la norma sitúa a la empresa en la posición de garante de un derecho que está directamente conectado con la salud del trabajador, por mor de los riesgos psicosociales asociados a la falta de descanso, y que, por tanto, le obliga, en virtud del art. 14.2, segundo párrafo, de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, a desarrollar *"una acción permanente de seguimiento de la actividad preventiva con el fin de perfeccionar de manera continua las actividades de identificación, evaluación y control de los riesgos que no se hayan podido evitar y los niveles de protección existentes"*.

Por todo ello, y si la empresa no cuenta con otra solución menos invasiva, podría estar justificado en estos casos que se realizasen registros rutinarios preventivos en los dispositivos digitales del trabajador para comprobar el cumplimiento de la exigencia de desconexión digital.

2.8 ¿Cuál podría ser un ejemplo de registro de ordenadores con la finalidad de comprobar la desconexión digital del trabajador?

La reciente incorporación a nuestro ordenamiento jurídico de la regulación del derecho de desconexión impide que, a día de hoy, contemos con pronunciamientos judiciales que nos sirvan de ejemplo. No obstante, es previsible que no tarde mucho en convertirse en conflicto la necesidad empresarial de constatar, mediante control del uso de los dispositivos digitales del trabajador, si éste ha respetado o no las directrices establecidas por la empresa al respecto, tanto en lo relativo a su intervención activa (no desconexión), como en cuanto a la de un tercero (normalmente, jefe de equipo) que haya intercedido en su derecho a la desconexión.

Sí encontramos, en cambio, ejemplos ya en algunos convenios colectivos recientes, que regulan el derecho a la desconexión digital de los trabajadores. Entre otros:

- El art. 73 del Convenio colectivo de Industria, Servicios e Instalaciones del Metal de la provincia de Madrid: *"Se fomentará la desconexión digital una vez finalizada la jornada laboral: no responder al teléfono, a los correos electrónicos o mensajes profesionales de cualquier otro tipo, etc. Fuera de su horario de trabajo"*.

- El art. 41 del Convenio Colectivo del sector de Abogados, Procuradores y Graduados Sociales de Cantabria 2019-2022: *"Las partes firmantes de este Convenio coinciden en la necesidad de impulsar el derecho a la desconexión digital una vez finalizada la jornada laboral. Por ello, salvo causa de fuerza mayor, se reconoce el derecho de los trabajadores a no responder a los e-mails o mensajes profesionales fuera de su horario de trabajo"*.

- El art. 23.3.4 del Convenio colectivo de Orange Espagne, SAU: *"... El derecho a la desconexión digital debe entenderse referido tanto a los períodos de vacaciones y permisos, como a los fines de semana, festivos y, en general, entre la finalización de la jornada laboral y el inicio de la siguiente. En los periodos de vacaciones y permisos, el empleado, para evitar cualquier tipo de incidencia, deberá programar una respuesta*

automática en la que, indicando su situación y las fechas en las que no estará disponible, designe el correo de contacto para la reasignación del servicio.

Orange recuerda que no hay obligación a responder durante estos períodos.

No resultará de aplicación esta política en aquellos supuestos en los que concurran causas de fuerza mayor, circunstancias excepcionales o un posible perjuicio empresarial que precise de respuesta inmediata.

Estas disposiciones serán de aplicación tanto a los empleados/as que prestan servicios de modo presencial como a los sujetos a régimen de teletrabajo, siempre y cuando no se encuentren en situación de guardia, disponibilidad, reten, o supuestos similares".

Incluso, existían ya ejemplos sobre la materia en convenios colectivos anteriores a la regulación legal de la desconexión digital:

- El art. 14 del Convenio colectivo del Grupo Axa (BOE 10-10-2017), una vez aclarada la perspectiva y los motivos por los cuales se reconoce el derecho de los trabajadores la desconexión digital, prevé que "salvo causa de fuerza mayor o circunstancias excepcionales, AXA reconoce el derecho de los trabajadores a no responder a los mails o mensajes profesionales fuera de su horario de trabajo".

- El Acuerdo Laboral de Fusión Santander-Popular-Pastor, de fecha 26 de junio de 2018, reconoce en su anexo IV, dedicado a los criterios para una ordenación racional del tiempo de trabajo, "el derecho de los profesionales para no responder a emails o mensajes profesionales fuera de sus horarios de trabajo, ni durante los tiempos de descanso, permisos, licencias o vacaciones, salvo causa de fuerza mayor o circunstancias excepcionales".

- También la empresa Telefónica ya firmó el 23 de noviembre de 2018 con los sindicatos CCOO y UGT un compromiso de impulsar medidas dirigidas a potenciar el respeto al tiempo de descanso de los trabajadores una vez finalizada la jornada laboral, reconociendo el derecho a la desconexión digital como elemento fundamental para lograr una mejor ordenación del tiempo de trabajo en aras del respeto de la vida privada y familiar y, en definitiva, de la calidad de vida y salud de los trabajadores. A la vez la empresa promoverá en sus diferentes territorios acciones de sensibilización / formación dirigidas a mandos y empleados a fin de informar sobre los riesgos, desafíos y buenas prácticas relación con el uso de las herramientas digitales. Todo ello se ha concretado en la Política interna reguladora del derecho a la desconexión digital de las personas trabajadoras de Telefónica, de 17 de julio de 2019.

c) Delimitación del debate procesal

2.9 ¿Qué significa doctrina de los frutos del árbol envenenado?

De acuerdo con este criterio –surgido de la doctrina judicial del orden jurisdiccional penal–, la ilicitud de una prueba (ilicitud derivada de que se obtuvo mediante injerencia en un derecho fundamental) contamina de nulidad a otras pruebas que, aunque lícitas, indirectamente se

obtuvieron gracias a la información o ventaja que procuró aquella prueba ilícita (conexión de antijuridicidad), es decir, que no tienen un origen independiente[6].

Este razonamiento se ha traído al ámbito laboral, pero no solo para expulsar del proceso a los otros medios de prueba que deriven de la prueba ilícita[7], sino también, por parte de algunos órganos jurisdiccionales, para declarar la nulidad de la medida empresarial, que se contaminaría también de esa ilicitud. Este alcance, sin embargo, hasta el momento no se admite unánimemente entre los Tribunales ni los autores[8].

2.10 ¿Existe una posición mayoritaria respecto a que la ilicitud de la prueba del registro de ordenadores conlleve la nulidad de la medida empresarial?

No, como recuerda la STSJ Cataluña 2402/2019, de 14 de mayo (Rec. 1618/2019), la cuestión no es en absoluto pacífica, y en la doctrina de suplicación podemos encontrar pronunciamientos opuestos de los diferentes Tribunales Superiores de Justicia.

Las sentencias que se sitúan a favor de la nulidad de la medida disciplinaria en estos casos, se apoyan en las SSTC 196/2004, de 15 de noviembre, y 29/2013, de 11 de febrero. En particular, la primera de ellas, en un supuesto en el que el trabajador demandaba por despido tras comunicársele la no superación del período de prueba, alegando que se había vulnerado su derecho a la intimidad al haberse basado la decisión extintiva en que se le realizó un reconocimiento médico en el que se constató consumo de drogas, la Sala señala que *«al 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, con vulneración por tanto del art. 18.1 CE, procedente será el otorgamiento del amparo, debiendo recordarse que, según constante doctrina de este Tribunal (entre otras, SSTC 38/1981, de 23 de noviembre, 114/ 1989, de 22 de junio, 186/1996, de 25 de noviembre, 1/1998, de 12 de enero, 57/1999, de 12 de abril, 20/2002, de 28 de enero, o 49/2003, de 17 de marzo),* ***la reparación de la lesión de un derecho fundamental que hubiese sido causado por el despido laboral, debe determinar la eliminación absoluta de sus efectos, es decir, la nulidad del mismo****, lo que implica la anulación de la Sentencia impugnada y declaración de la firmeza de la Sentencia del Juzgado de lo Social que con acierto aplicó el art. 18.1 CE* (y declaró la nulidad de la extinción)».

En esta línea, por ejemplo, se sitúan diversas sentencias y, entre las más recientes, podemos apuntar las siguientes:

---

[6] PRECIADO DOMÈNECH, CH., "Monitorización: GPS, Wearables y especial referencia a los controles biométricos para el registro horario. Aspectos procesales". Capítulo de la presente obra colectiva.

[7] De acuerdo con los arts. art.11.1 LOPJ, 90.2 LRJS y 287 LEC, no se admitirán ni valorarán las pruebas ilícitas, calificación que se reserva para aquellas obtenidas vulnerando derechos fundamentales. La justificación de este «efecto dominó» se encuentra, según dice la STS (Penal) de 18 de julio de 2002 (Rec. 3269/2000), en que solo de este modo se asegura que la prueba ilícita inicial no surta efecto alguno en el proceso. Si ésta ha sido obtenida mediante una actuación vulneradora de los derechos fundamentales, procede la anulación de su efectividad probatoria, y, como consecuencia del denominado «efecto dominó», que derriba y arrastra toda la prueba derivada de la vulneración constitucional, ello determina el decaimiento de todas las pruebas posteriores derivadas de ella.

[8] Como apunta FALGUERA BARÓ, MA. "Nuevas tecnologías y trabajo (y III): perspectiva procesal", Revista Trabajo y derecho: nueva revista de actualidad y relaciones laborales, Nº. 22, 2016, págs. 31-44, "…la referida doctrina tiene índole esencialmente penal, dónde el carácter inquisitivo del proceso comporta la lógica de que la prueba ilícita única extienda sus efectos sobre todas las actuaciones. Pero ello no tiene porqué ser así en los procesos dispositivos, máxime en los de índole verbal como el laboral…".

	HECHOS RELEVANTES	FALLO
STSJ Cataluña 1887/2018, de 22 de marzo (Rec. 255/2018)	*«…despido del trabajador, por trasgresión de la buena fe contractual, al haber consumido en el almacén en tres ocasiones productos caducados o en devolución por mal estado, sin haberlos pasado por caja, y haber fumado un cigarrillo en una de estas veces, lo que se probó a través del visionado de la grabación de la cámara del almacén, existiendo esta cámara y otras en las tiendas desde hacía más de diez años, comunicado en su día a la representación legal de los trabajadores, y, posteriormente, se dice a los trabajadores, en concreto al demandante…»*	Descartada la licitud de la prueba, concluye la Sala que *«…el despido, fundado en esta única prueba lesiva de derechos fundamentales, es nulo, en concordancia con los artículos 55.5 del Estatuto de los Trabajadores y 108.2 de la Ley Reguladora de la Jurisdicción Social ; por lo tanto, se estima el motivo en su primer apartado…».*
STSJ Cataluña 1726/2017, de 9 de marzo (Rec. 39/2017)	La trabajadora, encargada de esterilización, es objeto de despido disciplinario al imputarle determinados incumplimientos captados a través de dos cámaras ocultas instaladas durante 3 semanas.	*«…el Juzgador "a quo" anuda la nulidad del despido a la ilicitud de la prueba de videograbación, por haber sido obtenida con vulneración de derechos fundamentales, criterio que compartimos por cuanto dicha prueba era el único fundamento del despido de la trabajadora, por lo que debe declararse nulas todas las consecuencias de aquella prueba, como si de la teoría del " fruto del árbol envenenado" tantas veces aplicada en el ámbito penal se tratara y, así, del despido, al haberse producido " con vulneración de derechos fundamentales"…».*
STSJ Asturias 83/2016, de 22 de enero (Rec. 2404/2016)	*«El demandante era el encargado de la tienda que la empresa tiene abierta en… Gijón. Bajo su mando prestaban servicios varias trabajadoras, que en octubre de 2014 comunicaron a la demandada la comisión por aquél de irregularidades en el desempeño de sus funciones. Para investigarlas, la empresa entre otras medidas decidió instalar cámaras de video vigilancia… El demandante fue el único trabajador de la tienda ignorante de la colocación de ambos sistemas de video vigilancia, los cuales junto con la colaboración de un detective privado fueron utilizados para observar y dejar constancia de las actuaciones imputadas en la carta de despido»*	*«El incumplimiento por la empresa del deber informativo supuso una violación de los derechos fundamentales del demandante afectados por la medida intrusiva. Y aunque la recurrente quiere limitar la consecuencia de su infracción a la validez del medio de prueba obtenido con la grabación de imágenes realizada, la nulidad del despido constituye el efecto necesario y adecuado de la actuación empresarial. Conforme dispone el art. 55.5 del Estatuto de los Trabajadores el despido es nulo cuando tenga por móvil alguna de las causas de discriminación prohibidas por la Constitución o en la Ley, o bien se produzca con violación de derechos fundamentales y libertades públicas del trabajador»*
STSJ País Vasco 609/2013, de 9 de abril (Rec. 445/2013)	Se combate *«el despido que acordó* (la) *empresa de su trabajadora doña Mariola por razones disciplinarias* *con efectos del día 19 de octubre de 2011, imputándole haber realizado una serie de conductas irregulares en* *su actividad como cajera de un supermercado de dicha empresa»*, todo ello con base en una grabación obtenida con el sistema de videovigilancia de la empresa	*«Consecuencia de lo anterior, es que el recurso deba ser desestimado en su integridad, confirmando la nulidad del despido actuado en base a uso ilegítimo de medios de control de la actividad de la trabajadora, conculcadores del mencionado derecho fundamental al control de los datos personales de la trabajadora demandante, tal y como hizo el Juzgador, que al efecto cita la sentencia del Tribunal Constitucional 196/2004, de 15 de noviembre, en tesis que implícitamente se mantiene en la sentencia 29/2013 ya citada al anularse la sanción, siguiendo otros precedentes de tal Tribunal, como las sentencias 49/2003, de 17 de marzo y 20/2002, de 28 de enero»*
STSJ País Vasco de 10 de mayo de 2011 (Rec. 644/2011)	*«La decisión extintiva se fundó en que la conducta del actor durante los días 25, 26 y 28 de junio y 1 y 3 de julio de 2010 -fechas en las que se encontraba en situación de incapacidad temporal a causa de un dolor en el brazo izquierdo, iniciada el 17 de junio de ese mismo año-, consistente en realizar actividades similares a las efectuadas para la empresa (conducir su vehículo particular de manera habitual y durante varias horas al día, desplazarse a pie y transportar bolsas de la compra en varias ocasiones, y llevar sendos*	*«Dado que la única prueba que sirvió de base al acto extintivo fue obtenida violando el derecho fundamental a la intimidad del demandante y que, por lo tanto, el conocimiento de los hechos motivadores de su cese se debió en exclusiva a una prueba ilícitamente obtenida, con vulneración de esa garantía constitucional, la consecuencia que de ello deriva es la nulidad del despido de conformidad con lo preceptuado en el primer párrafo del apartado 5 del artículo 55 del Estatuto de los Trabajadores y en el artículo 108.2 de la Ley de Procedimiento Laboral, que establecen que será*

	equipajes de viaje en el último de los días señalados), entraña una transgresión de la buena fe contractual, así como una deslealtad y un abuso de confianza… (E)*l único elemento probatorio aportado por la demandada para acreditar los hechos imputados en la carta de despido -el informe elaborado por el (detective) y la declaración que prestó en el acto de juicio- se sustenta en la instalación y posterior utilización de un localizador GPS en el vehículo privado del actor, sin garantía alguna…»*.	*nulo el despido que se produzca con violación de derechos fundamentales y libertades públicas del trabajador. Atendiendo a criterios gramaticales, finalistas y de interpretación conforme a la Constitución, en la citada previsión legal encuentran cobijo no solo los supuestos en que el cese se produce como consecuencia del ejercicio legítimo de un derecho fundamental, sino también aquellos otros en que los hechos que lo sustentan han sido conocidos por el empresario mediante métodos que conculcan los derechos fundamentales del afectado.* *A favor de esa solución se decanta la sentencia 196/2004, de 15 de noviembre, del Tribunal Constitucional, examinando una decisión extintiva fundada en la ineptitud de la recurrente para el trabajo conforme a los resultados de un reconocimiento médico atentatorio a su intimidad, por entender que "la reparación de la lesión de un derecho fundamental que hubiese sido causado por el despido laboral, debe determinar la eliminación absoluta de sus efectos, es decir, la nulidad del mismo"»*.

Frente a este posicionamiento, otras Sentencias consideran, en cambio, que la no admisión del medio de prueba obtenido ilícitamente no conduce a que la decisión extintiva, en sí misma considerada, pretendiera la vulneración de derechos fundamentales del trabajador, que permitiría la calificación de despido nulo conforme al art. 55 ET. Entre estas Sentencias, se encuentra, por ejemplo, las siguientes:

	HECHOS RELEVANTES	FALLO
STSJ Madrid nº 597/2018, de 13 de septiembre (Rec. 417/2018)	Ante la sospecha de que por el trabajador (vigilante de seguridad) *«…no estuviera siendo cumplida la instrucción impartida por la empresa en orden a las llamadas requisas, controles de seguridad aleatorios de vehículo en accesos al recinto y a los estacionamientos públicos que han de efectuar los vigilantes de seguridad de Securitas mediante la cumplimentación de un documento impreso en el que deben dejar constancia del nombre, evento durante el cual se realiza el control, fecha, hora, puesto, matrícula, marca y modelo del vehículo objeto de control. Por ello, se procedió al visionado de las imágenes de las cámaras instaladas en aparcamientos y entradas de vehículos al recinto y que enfocan sus accesos, pudiéndose comprobar que un total de quince vigilantes de seguridad, entre ellos el ahora demandante, registraban en el impreso como ejecutados controles de vehículos que no constaba en dichas imágenes que se hubieran realizado…»*.	Previa consideración de que las grabaciones de las cámaras de seguridad fueron ilícitamente obtenidas, la Sala declara la improcedencia del despido, aclarando que *«…no procede la calificación de despido nulo, puesto que no se ha probado que la decisión extintiva acordada por la empresa demandada, en si misma considerada, pretendiera la vulneración de derechos fundamentales o libertades públicas del trabajador recurrente, ni que el móvil del empresario al acordar el despido respondiera a una causa vulneradora de esos derechos fundamentales lo que legalmente llevaría aparejada la nulidad del despido, cuestión distinta de la sucedida en este supuesto en que el empresario, al intentar comprobar el comportamiento del trabajador y obtener pruebas de sus incumplimientos para tratar de justificar un despido, ha obtenido de forma ilícita tal prueba con vulneración de derechos fundamentales de su empleado, no pudiendo de esta manera confundirse el despido con violación de derechos fundamentales con la infracción de derechos fundamentales para la obtención de la prueba de los hechos en los que se basó la empleadora para adoptar tal sanción…»*.
STSJ de Castilla-La Mancha (Albacete) nº 25/2018, de 12 de enero (Rec. xxx)	*«…En la carta* (de despido entregada al trabajador, vigilante de seguridad) *se alude a que, pese a haber sido amonestado verbalmente, continúa fumando en las instalaciones* (…) *Asimismo, se le imputa una disminución voluntaria y continuada en el rendimiento en su puesto de trabajo, la comisión de actos inmorales en el puesto de trabajo, tales como, visionado de*	*«…no existen razones de peso suficientes para alterar el ámbito de aplicación del artículo 55.5 ET, en tanto en cuanto pensamos que la sanción de nulidad del despido tiene su fundamento en el móvil del empresario cuando el despido en sí mismo responde a una causa vulneradora del derecho fundamental, pero no cuando la finalidad que mueve al empresario es comprobar un*

	material pornográfico y masturbaciones en el trabajo, y distracciones graves por juegos o conversaciones telefónicas…».	*comportamiento del trabajador para obtener la prueba de la existencia de la causa alegada para justificar el despido, en cuyo caso procede la nulidad de dicha prueba obtenida con vulneración de derechos fundamentales, sin que tal nulidad pueda extenderse a la calificación del despido que podrá ser improcedente o incluso procedente, si una vez desechados los hechos acreditados mediante la prueba ilegal o ilegítima, aún resultan probados, mediante prueba hábil e idónea, hechos que constituyen un incumplimiento grave y culpable del trabajador…».*
STSJ Madrid. 1033/2015, de 28 de junio (Rec.)	Se analiza el caso de una trabajadora despedida, habiendo empleado a tal efecto la empresa grabaciones de vídeo de la trabajadora.	*«…Tampoco puede acogerse la pretensión de la actora, ya que para que el despido sea nulo, conforme a lo dispuesto en el artículo 108.2 de la citada Ley rituaria, es necesario que tenga como móvil alguna de las causas de discriminación previstas en la Constitución y en la ley, o se produzca con violación de derechos fundamentales y libertades públicas del trabajador, o que éste se encuentre en alguno de los supuestos prevenidos en el apartado segundo de dicho precepto en los que no se halla la trabajadora, sin que tampoco exista indicio alguno de que la extinción contractual haya tenido como móvil causa alguna de discriminación ni se haya producido con violación de sus derechos o libertades, confundiendo la recurrente el despido vulnerador de éstos, con la infracción de los mismos para la obtención de la prueba de los hechos en los que se fundamenta, cuestiones absolutamente diferentes, ya que para que el despido sea nulo ha de producirse por una causa ajena al contrato de trabajo, directamente atentatoria contra un derecho fundamental y verdadero móvil de la decisión extintiva del empleador, absolutamente al margen de cualquier motivo disciplinario…».*

Aunque las sentencias indicadas no aluden ninguna a un supuesto de registro de dispositivos digitales, sus conclusiones son perfectamente aplicables al mismo.

En definitiva, estamos ante un debate procesal complejo, superado por una realidad que puede resultar muy variada merced a elementos diferenciadores tales como (i) que nos encontremos ante una medida disciplinaria pluricausal o no; o (ii) que la medida empresarial aporte como único medio de prueba la información obtenida del registro del ordenador o cuente con otros medios probatorios ajenos a dicho registro, es decir, que se hayan utilizado como otras vías de comprobación de la sospecha al margen por completo del examen del dispositivo digital. Todo ello puede conducir a respuestas judiciales diversas en este punto.

3. DIMENSIÓN CONSTITUCIONAL: SUS PARÁMETROS DE LICITUD

Tal y como venimos advirtiendo, la trascendencia del registro empresarial del ordenador o de otros dispositivos digitales facilitados al trabajador, reside en su potencial vulneración de derechos fundamentales del trabajador, dado que tales dispositivos, aun destinados al desempeño de las funciones laborales, son susceptibles siempre de un uso privado, incluso aunque éste se prohíba por la empresa. De ahí que expresamente haya tenido que reconocerse

que los trabajadores tendrán derecho a la protección de su intimidad[9] en el uso de los dispositivos digitales puestos a su disposición por su empleador (art. 20.bis ET y art. 87.1 LOPDGDD) y que se recuerde también este límite cuando se alude genéricamente a que la empresa deberá guardar "la consideración debida a (la) dignidad" del trabajador (art. 20.3 ET).

La empresa deberá observar, por tanto, una conducta compatible con el respeto del contenido esencial de los derechos fundamentales amenazados. La concreción de las pautas de actuación empresarial acordes con esta exigencia, que determinarán la validez del registro, empiezan su andadura en la doctrina del TC.

3.1 ¿Qué derechos fundamentales están en juego?

Está en juego el art. 18.1 CE, relativo a la intimidad personal, y estamos ante la posible afectación del secreto de las comunicaciones (art. 18.3 CE) y de la protección de la intimidad informática y los datos de carácter personal (18.4 CE). Derechos fundamentales que deben equilibrarse con el poder de dirección del empresario, imprescindible para la buena marcha de la organización productiva (organización que refleja otros derechos reconocidos constitucionalmente en los arts. 33 y 38 CE), poder reconocido expresamente en el Art. 20 ET, que atribuye al empresario, entre otras facultades, la de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales, respetando la dignidad del trabajador (arts. 4.2.c. y 20.3 ET).

En definitiva, podemos resumir este conflicto de derechos fundamentales afirmando que la empresa se topa con un **trabajador invisible** (porque aspira a preservar su esfera personal también en el trabajo) cuando lo que preferiría encontrar, como titular de los medios de producción, es un **trabajador transparente** (porque querría acceder al rastro de toda su actividad). Se trata de un conflicto laboral radical.

3.2 Los derechos fundamentales afectados por el registro del ordenador ¿son un límite infranqueable que impide cualquier registro?

No. Aunque tales derechos son plenamente aplicables al ámbito de las relaciones laborales, sabemos que los mismos no operan como derechos absolutos, de manera que pueden ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquéllos hayan de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho (entre muchas otras, SSTC 57/1994, FJ 6, y 143/1994, FJ 6).

3.3 Las facultades de vigilancia y control que confiere el art. 20.3 ET ¿permiten entonces a la empresa un examen ilimitado de sus dispositivos digitales puestos a disposición de los trabajadores?

No. Tales facultades no amparan intromisiones ilegítimas de la empresa en la intimidad de sus trabajadores en los centros de trabajo.

En efecto, aunque el ejercicio de los derechos fundamentales del trabajador admita limitaciones o sacrificios por estar desenvolviéndose en el seno de una organización (la empresarial), que

[9] Olvida la Ley mencionar también el derecho al secreto de las comunicaciones (art. 18.3 CE) y el derecho a la protección de datos de carácter personal (art. 18.4 CE)

es reflejo de otros derechos reconocidos constitucionalmente (libertad de empresa) (STC 90/1997), ello solo cabe en situaciones extremas en las que la limitación del derecho fundamental se presenta como imprescindible para el correcto y ordenado desenvolvimiento de la actividad empresarial (STC 99/1994)[10].

3.4 ¿Podría la empresa, como alternativa, eliminar la presencia de tales derechos fundamentales en la empresa prohibiendo completamente el uso privado de los ordenadores y otros dispositivos digitales?

Aunque, en este punto, la doctrina de los Tribunales españoles ha admitido esta posibilidad, consideramos que ello es dudoso porque, si bien los derechos fundamentales no son absolutos, debe considerarse excepcional que puedan "reducirse a cero". En este sentido, podemos ya adelantar que serían cuestionables los códigos de conducta de las empresas que introducen la regla de tolerancia cero en el uso personal de los medios de la empresa.

Tal y como señalamos en la siguiente pregunta, y en las preguntas 18 y 33 del presente texto, el hecho de que la empresa "cumpla rigurosamente las reglas del juego" relativas a los usos permitidos del ordenador ex art. 18.3 CE, prohibiendo su uso privado, no supone que deba entenderse superado el art. 18.1 CE que solo permitiría tal limitación absoluta si está justificado en términos de proporcionalidad y, por tanto, entendemos que con carácter muy excepcional.

Incluso en el caso de que se considerase válida esta posición jurídica, no sería muy recomendable, desde la perspectiva de la gestión de recursos humanos o de personas, una política como ésta, de prohibición radical de cualquier uso privado, totalmente contraria a la realidad social, toda vez que difícilmente contribuya a captar y retener el talento: ¿qué trabajador de un nivel profesional medio, medio-alto o alto, estaría dispuesto a trabajar en una entidad empresarial que prohíbe sin más matización el uso privado del ordenador pudiendo activarse el régimen sancionador en caso de incumplimiento?

3.5 ¿Cuándo incurrirá la empresa en una intromisión ilegítima en los derechos fundamentales del trabajador al registrar su ordenador u otro dispositivo digital facilitado para su trabajo?

Partiendo de la inevitabilidad del potencial uso privado del ordenador de la empresa, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales –como puede ser el registro de este tipo de dispositivos– vendrá determinada por la estricta observancia del principio de proporcionalidad.

Así, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto). Reitera así una doctrina clásica que ya desarrolló en las SSTC 66/1995, de 8 de mayo, FJ 5; 55/1996, de 28 de

[10] PEDRAJAS QUILES, A. "Derechos fundamentales de la persona, del trabajador y autonomía privada", en Libro homenaje a Abdón Pedrajas Moreno, coord. por Tomás Sala Franco, 2012, págs. 403-424.

marzo, FFJJ 6, 7, 8 y 9; 207/1996, de 16 de diciembre, FJ 4 e), y 37/1998, de 17 de febrero, FJ 8.

3.6 ¿Es suficiente para determinar la licitud del registro empresarial la aplicación estricta del indicado principio de proporcionalidad?

No. Además, el TC ha añadido, en el enjuiciamiento de la colisión de las facultades de control de la empresa con el derecho a la intimidad de los trabajadores, la exigencia de respetar el derecho de autodeterminación informativa que consagra el artículo 18.4 CE[11].

Concretamente, a partir de las SSTC 29/2013 y 39/2016 (referidas a supuestos de video vigilancia) se consagra que el deber de información previa al trabajador es exigible también cuando el control empresarial incide en el derecho a la intimidad personal (art. 18.1 CE), y no solo cuando está en juego el derecho a la protección de datos de carácter personal (art. 18.4 CE). Se argumenta que, no obstante la doctrina de la STC 186/2000[12], el art. 18.1 CE impone como regla de principio y, de forma añadida al resto de sus garantías, un deber de información que protege frente a intromisiones ilegítimas en la intimidad. Advierte, además, la Sala que no exime de ese deber informativo al trabajador el interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia[13].

Aunque difieren ambas SSTC en el alcance de ese deber informativo referido a la instalación de cámaras de videovigilancia[14], el TC establece de esta manera un nuevo parámetro de licitud al registro de dispositivos digitales consistente en el cumplimiento de las exigencias derivadas del respeto del contenido esencial del derecho en materia de protección de los datos de carácter personal[15].

---

[11] El siguiente análisis (y sus notas al pie) acerca de esta evolución de la doctrina del TC se ha extractado de la Sentencia núm. 52/2019, de 18 de febrero, del JS núm. 3 Pamplona.

[12] En contra del nuevo criterio del TC, el FJ 7 de la STC 186/2000 señalaba que «[e]*l hecho de que la instalación del circuito cerrado de televisión no fuera previamente puesta en conocimiento del Comité de empresa y de los trabajadores afectados (sin duda por el justificado temor de la empresa de que el conocimiento de la existencia del sistema de filmación frustraría la finalidad apetecida) carece de trascendencia desde la perspectiva constitucional*».

[13] Considera la STC 29/2013 que *«esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, en su núcleo esencial. En efecto, se confundiría la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art. 20.3 ET en relación con el art. 6.2 LOPD/1999) con la constitucionalidad del acto (que exige ofrecer previamente la información necesaria, art. 5LOPD/1999), cuando lo cierto es que cabe proclamar la legitimidad de aquel propósito (incluso sin consentimiento del trabajador, art. 6.2 LOPD/1999) pero, del mismo modo, declarar que lesiona el artículo18.4 CE la utilización para llevarlo a cabo de medios encubiertos que niegan al trabajador la información exigible»*.

[14] La doctrina de la STC 29/2013 (que impone como necesaria una información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que la captación podía ser dirigida, en línea con lo que posteriormente se ha introducido en el art. 89 LOPDGDD, LO 3/2018) fue modificada en la STC 39/2016, de 3 de marzo. En efecto, el TC desestimó, en este caso, el recurso de amparo, delimitando el alcance del deber informativo a los trabajadores, que considera cumplido cuando la empresa coloca los distintivos informativos en las condiciones que establece la Instrucción 1/2006, de 8 de noviembre, de la AEPD.

[15] Criterio plenamente alineado con la concepción amplísima de las nociones de dato personal y tratamiento que se contiene en el art. 4 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), conforme a la cual difícilmente puede considerarse que la información a la que se accede en el control empresarial de los medios tecnológicos e informáticos que utilizan los trabajadores no constituya, cabalmente, un "dato personal" y que tal actividad sea, al mismo tiempo, "tratamiento". De la misma forma que la imagen -

En definitiva, la validez de la prueba derivada del registro empresarial de dispositivos digitales facilitados al trabajador requiere, desde el punto de vista constitucional, haber informado previamente a los trabajadores acerca de dicho control, su alcance y finalidad, como exigencia derivada del contenido esencial de los derechos a la intimidad y a la protección de datos de carácter personal.

4. LOS PARÁMETROS LEGALES DE LICITUD

Junto a las pautas de actuación empresarial que fija el TC en relación con el registro de dispositivos digitales utilizados por los trabajadores en el desarrollo de su prestación laboral, se encuentran las que concreta o añade la Ley (orgánica), a la que la Constitución hace el encargo de fijar los límites a los derechos fundamentales, sometida –eso sí– a la exigencia de que si introduce recortes, los mismos sean necesarios para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, respetuoso con el contenido esencial del derecho fundamental restringido[16].

En este sentido, son de inevitable referencia la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), así como el 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 sus datos personales (RGPD).

4.1 ¿Existe una previsión específica en la LOPDGDD en materia de registro de ordenadores y otros dispositivos digitales?

Sí. En relación con el control de dispositivos digitales, el art. 87 trata de fijar el punto de equilibrio entre los derechos en juego, mediante un reconocimiento expreso, por un lado, del derecho a la intimidad de los trabajadores en el uso de dispositivos digitales en el ámbito laboral (que también traslada al nuevo art. 20.bis ET) y, por otro lado, de las facultades de control de la empresa sobre estos dispositivos, si bien en los términos y con los límites que fije la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales. El indicado precepto concreta así el encargo a los Estados de la UE que realiza el art. 88 RGPD.

4.2 ¿Qué alcance debe atribuirse a tan trascendental reconocimiento expreso del derecho a la intimidad de los trabajadores en el uso de los dispositivos digitales en el ámbito laboral?

sistemas de videovigilancia- constituye un dato personal, también lo es la información a la que se accede cuando se controla la navegación por Internet, los ordenadores y los correos electrónicos La consecuencia jurídica no es otra que extender al control empresarial de los medios tecnológicos las mismas exigencias que el Reglamento europeo -sin excepción alguna aplicable a las relaciones laborales-, impone al tratamiento de los datos personales. Como sabemos, entre dichas exigencias se encuentra la transparencia en el tratamiento y el deber informativo previo a realizar la actividad.

[16] SSTC 57/1994, de 28 de febrero, FJ 6; 18/1999, de 22 de febrero, FJ 2, y en relación con el derecho a la protección de datos personales, STC 292/2000, FFJJ 11 y 16

Tan importante mención conlleva dos importantes pautas de actuación para la empresa en orden al ejercicio de su facultad de registro de los ordenadores[17]:

1) Que, con carácter previo al acceso y examen de dispositivos digitales del trabajador, la empresa deberá siempre analizar y excluir la posibilidad de utilizar medidas de prevención o de servirse de otras soluciones no tecnológicas, menos invasivas, que eviten el riesgo de afectación del derecho fundamental del trabajador (observancia del principio de necesidad).

2) Que, incluso en el caso de que la empresa haya prohibido expresa y totalmente el uso privado de los dispositivos digitales que ponga a disposición de los trabajadores, ello no neutralizará plenamente toda expectativa razonable de privacidad. En palabras de la STEDH 05-09-2017 (Bărbulescu II, parágrafo 80), *«las instrucciones de una empresa no pueden anular el ejercicio de la privacidad social en el puesto de trabajo. El respeto a la privacidad y confidencialidad de las comunicaciones sigue siendo necesario, aunque pueda limitarse dentro de las medidas de necesidad»*.

Como señalábamos anteriormente, los códigos de conducta que incorporen la regla de tolerancia cero en relación con el uso privado de los ordenadores de la empresa, es muy dudoso que liberen a la empresa de seguir las pautas de actuación acordes con el respeto de un derecho a la intimidad que, pese a la prohibición, no habrá dejado de estar presente. En este sentido, como veremos, la doctrina de los Tribunales españoles debería revisarse en este punto.

4.3 ¿Cuáles son las pautas de actuación empresarial que establece el art. 87 LOPDGDD para que el registro de los dispositivos digitales sea válido?

(i) El acceso por la empresa a las informaciones derivadas del uso de dispositivos digitales por los trabajadores y su tratamiento (como datos personales que son) solo cabrá en dos supuestos (que constituyen sus únicas bases jurídicas posibles de licitud):

- O bien "a los solos efectos de controlar el cumplimiento de las obligaciones laborales", incluido el reciente derecho a la desconexión, lo que limita el registro al control de las obligaciones de naturaleza laboral y no otras (6.1.b RGPD: tratamiento necesario para la ejecución de un contrato).

- O bien para "garantizar la integridad de dichos dispositivos", esto es, para salvaguardar la seguridad de los equipos y la red informática de la empresa y evitar la fuga de datos personales de trabajadores, clientes, etc. (6.1.f RGPD: tratamiento necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero)

(ii) La empresa solo podrá acceder unilateralmente a los dispositivos digitales facilitados a sus trabajadores si previamente ha cumplido con el deber legal de establecer sus criterios de utilización en el ámbito de la empresa, plasmados en los correspondientes Códigos de Conducta o protocolos de uso de medios

[17] BAZ RODRÍGUEZ, J. "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático". Trabajo y derecho: nueva revista de actualidad y relaciones laborales, núm. 54, 2019, págs. 49-78.

electrónicos[18], que –para ser suficientes a efectos de licitud de la prueba obtenida– deberán cumplir las siguientes exigencias:

- Respetar en todo caso los estándares mínimos de protección de la intimidad, de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente

- Haberse elaborado con la participación de los representantes legales de los trabajadores

- Haber establecido los usos privados autorizados de modo preciso, evitando equívocos o imprecisiones

- Haberse comunicado a los trabajadores, en cumplimiento así del deber de información y transparencia que requieren los derechos fundamentales en juego

4.4 ¿Serían válidas las cláusulas contractuales firmadas por el trabajador en su contrato en cuya virtud autorizase a la empresa a la instalación de aplicaciones que permitiesen el registro de la actividad del ordenador?

No. El art. 87 LOPDGDD únicamente contempla dos bases posibles de legitimación, de entre las que figuran en el RGPD, para el acceso y tratamiento por la empresa de los datos contenidos en los dispositivos digitales, a saber, el seguimiento de la ejecución del contrato y la satisfacción de intereses legítimos de la empresa o de terceros (arts. 6.1.b y 6.1.f RGPD), pero no el consentimiento del trabajador, que regula el art. 6.1.a) RGPD, y que no se incluye en el art. 87 LOPDGDD[19].

4.5 ¿Quedaría legitimada la empresa, mediante el citado art. 87 LOPDGDD, para reutilizar la información obtenida mediante el registro/monitorización de los dispositivos digitales que utiliza el trabajador?

No. El art. 87.2 LOPDGDD autoriza el acceso y tratamiento de los contenidos derivados del uso de medios digitales facilitados a los trabajadores, "a los solos efectos" de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos

[18] Se eleva así a la categoría de deber legal el que, hasta la fecha, constituía un criterio judicial sobre el que unificó doctrina la STS (Social) 26-09-2007 (RCUD 966/2006), en cuyo FJ 4º, señalaba que *«lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones»*. Este criterio era acorde con el de la STEDH 03-09-2007 (asunto Copland vs Reino Unido), si bien entonces, la referencia a la existencia de tales reglas de uso se señalaba a los efectos de eliminar con ello la expectativa de privacidad del trabajador, lo que, según aquel criterio, permitiría a la empresa, si había prohibido el uso privado de los dispositivos digitales, realizar un control integral de sus dispositivos digitales, puesto que, existiendo tal advertencia, no podría hablarse de intromisión en la intimidad del trabajador. Esta interpretación, como hemos señalado, quedaría ahora inhabilitada merced al reconocimiento expreso del derecho a la intimidad del trabajador en el uso de los dispositivos digitales en el ámbito laboral que recoge el art. 87.1 LOPDGDD.

[19] BAZ RODRÍGUEZ, J. "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático". Trabajo y derecho: nueva revista de actualidad y relaciones laborales, núm. 54, 2019, págs. 49-78.

dispositivos. No se contempla ningún otro uso por la empresa más allá de dicha finalidad, y ello aunque el art. 6.4 RGPD dé cabida a otros fines distintos[20].

Incluso aunque la empresa cumpliese con la exigencia del art. 64.5.III, f) ET y requiriese el informe previo de la representación legal de los trabajadores, el uso secundario de la información obtenida mediante el control de los dispositivos digitales facilitados a los trabajadores entraría en conflicto con el derecho a la protección de datos de carácter personal.

4.6 ¿Sería válida la prueba obtenida unilateralmente mediante el registro de ordenadores en la empresa que no disponga criterios de utilización?

No. No obstante, en opinión de algunos autores[21], si la empresa carece de código de conducta al efecto, cabría en estos casos acudir al art. 90.4 LRJS, solicitando autorización judicial para acceder al ordenador del trabajador, a fin de obtener válidamente prueba de la infracción laboral

4.7 A qué se refiere el art. 87.3 LOPDGDD cuando requiere que, en la elaboración de los criterios de utilización de los dispositivos digitales, deberán "participar" los representantes de los trabajadores

Llama la atención que el TEDH haya puesto el foco siempre en la información a los trabajadores y no a la RLT. La LOPDGDD, sin embargo, introduce este requisito, aunque sin suficiente concreción, pues no especifica el tipo de "participación" que será suficiente.

Podemos entender que, salvo que el convenio colectivo concrete otro alcance, participación aquí podría equivaler a dos posibles intensidades:

- O bien a la que ya le reconoce el art. 64.5.III, f) ET, que implica ser informada y tener la ocasión de emitir informe previo al respecto, preceptivo, pero no vinculante.

- O bien a "consulta", en el sentido de ponerse en contacto con la RLT para recabar e intercambiar opiniones, para compartir información que permita resolver conjuntamente la necesidad planteada.

Pero, en ningún caso, entendemos que equivalga a la exigencia de abrir un proceso de negociación, que impone un intercambio de propuestas y ceder cada cual en las propias en pos de un acuerdo.

4.8 ¿Sería válida la prueba obtenida aun disponiendo de criterios de uso de dispositivos digitales, pero en cuya elaboración no haya participado la representación legal de los trabajadores (RLT) o lo haya hecho sin respetar la empresa las exigencias de la buena fe (por ejemplo, sin facilitarles información suficiente para emitir opinión/informe)?

[20] BAZ RODRÍGUEZ, J. "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático". Trabajo y derecho: nueva revista de actualidad y relaciones laborales, núm. 54, 2019, págs. 49-78.

[21] BAZ RODRÍGUEZ, J. "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático". Trabajo y derecho: nueva revista de actualidad y relaciones laborales, núm. 54, 2019, págs. 49-78.

El incumplimiento de tal exigencia de participación de la RLT podría quedarse en las consecuencias meramente sancionadoras para la empresa, por aplicación de la LISOS. Sin embargo, debemos inclinarnos por considerar que, en tal caso, las reglas de uso establecidas para el uso de dispositivos digitales no cumplirían plenamente con las exigencias legales, por lo que, aunque se respetasen, serían insuficientes para otorgar licitud a la prueba obtenida.

4.9 ¿Qué sucede si no existen en la empresa representantes legales de los trabajadores a los que hacer participar para la elaboración de los criterios de utilización de dispositivos digitales?

La Ley no resuelve esta hipótesis, si bien, en tal caso, debemos entender que no quedaría eximida la empresa de elaborar tales criterios de utilización, que no dejarían de estar sometidos al resto de exigencias legales, en el sentido de ser conformes con los usos sociales y los derechos reconocidos constitucional y legalmente; expresar sin ambigüedades los posibles usos privados autorizados y haberse informado de los mismos con carácter previo a los trabajadores.

4.10 ¿Qué sucede si existe representación legal de los trabajadores en unos centros de trabajo y en otros no?

Ninguna respuesta nos da el art. 88 LOPDGDD, siendo un ejemplo más –sólo uno más– de la necesidad de que, antes o después, se aborde una revisión profunda de la legitimidad negocial en el banco social cuando estamos ante decisiones empresariales de dimensión colectiva.

A falta de especificación o reforma, lo recomendable en estos casos pasaría por acudir a los criterios de negociación del convenio colectivo ex título III del ET y no, desafortunadamente, a las modalidades más versátiles de negociación dispuesta en los artículos 40, 41 o 47 del ET.

4.11 ¿Sería válida la prueba obtenida mediante el registro de dispositivos digitales sin haber informado previa y suficientemente a los trabajadores acerca de sus reglas de uso?

No. El art. 87.3, in fine, LOPDGDD es contundente en el sentido de establecer que "los trabajadores deberán ser informados de los criterios de utilización".

5. EVOLUCIÓN JUDICIAL EN RELACIÓN CON LOS PARÁMETROS DE LICITUD DEL REGISTRO DE LOS DISPOSITIVOS DIGITALES

Para completar los límites a la facultad empresarial de registro de los ordenadores y otros dispositivos digitales facilitados por la empresa a los trabajadores, es imprescindible la concurrencia del criterio de los Tribunales. Su recorrido previo a la LOPDGDD y el sometimiento a la doctrina del TEDH han marcado una evolución en la que no siempre coinciden los posicionamientos de los Tribunales nacionales y del Tribunal europeo.

En este sentido, existe un claro punto de inflexión reciente en la STEDH de 05-09-2017 (asunto Bărbulescu-II), que establece las últimas pautas de la actuación empresarial en esta materia.

a) <u>Etapa pre-Bărbulescu II</u>

5.1 ¿Cuál era la posición de los tribunales antes de Bărbulescu-II?

Con la STS (Social) 26-09-2007 (RCUD 966/2006) quedó atrás en España aquella postura inicial de una parte de la doctrina que situaba el registro empresarial del ordenador en el ámbito del art. 18 ET y, por tanto, sujeto a sus garantías[22]. Dejó claro la Sala que el ordenador u otros dispositivos digitales son instrumentos de producción cuya titularidad corresponde a la empresa "como propietario o por otro título" y ésta tiene, por ello, facultades de control de la utilización, que incluyen lógicamente su examen. Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento.

En este punto, para el control de los dispositivos digitales, tanto el TC como el TEDH venían exigiendo **eliminar la expectativa de intimidad o secreto** que pudiera tener el trabajador, imponiendo a la empresa un deber informativo a los trabajadores sobre la existencia del control empresarial y los medios utilizados. Por ejemplo, la STEDH 03-04-2007, Copland vs. Reino Unido, afirmaba que la expectativa de intimidad y confidencialidad de los trabajadores solo desaparece si la empresa advierte de la fiscalización (en el mismo sentido las SSTS, Social, 26-09-2007, RCUD 966/2006, y 08-03-2011, RCUD 1826/2010).

No obstante, la jurisprudencia previa del TS, que acoge sin excepción la doctrina del TEDH, en la posterior STS (Social) 06-10-2011, RCUD 4053/2010**, había introducido una excepción al deber informativo previo cuando no existe tolerancia empresarial** en el uso por los trabajadores de los medios tecnológicos o informáticos para usos particulares y se ha establecido una regla de prohibición absoluta. Razonaba así la Sala que, aunque la STS de 26-09-2007 exigía informar a los trabajadores de la existencia de control empresarial y los medios utilizados, esta concreta exigencia la calificaba de mero "obiter dicta", que **no era aplicable en supuestos de prohibición absoluta** del uso de los medios tecnológicos en los que no concurre expectativa alguna de confidencialidad o intimidad por parte de los trabajadores que haya podido ser sorprendida con la actuación fiscalizadora de la empresa. En el mismo sentido cabe citar la STC 170/2013, de 7 de octubre, para un supuesto en el que el convenio colectivo tipificaba como infracción los usos extra laborales de las herramientas informáticas, considerando que esta previsión implicaba una prohibición expresa que conllevaba la facultad de la empresa para controlar la utilización de las herramientas informáticas sin necesidad de previa información a los trabajadores[23].

Posteriormente, sin embargo, como hemos señalado en la pregunta 16 del presente capítulo, con las SSTC 29/2013 y 39/2016 la doctrina del TC introdujo la exigencia del deber de información previa al trabajador, pero no ya para excluir cualquier expectativa de intimidad, sino como exigencia derivada del respeto del derecho a la protección de datos de carácter personal.

5.2 ¿Se han encontrado siempre alineadas la jurisdicción social y penal en esta materia?

No plenamente. Tal y como recuerda la STS (Penal) 23-10-2018 (Rec. 1674/2017), *«la extensión que deba conferirse a las facultades de supervisión del empresario en el marco de una relación laboral y, en concreto, si está habilitado para verificar el uso que da uno de sus*

[22] La citada Sentencia, en su FJ 3º, ofrece cumplida explicación de las razones por las que el art. 18 ET no es aplicable al control por el empresario de los medios informáticos que se facilitan a los trabajadores para la ejecución de la prestación laboral.

[23] Resumen extractado de la Sentencia núm. 52/2019, de 18 de febrero, del JS núm. 3 Pamplona.

empleados a los dispositivos informáticos o aquellos otros aptos para comunicaciones puestos a su disposición es cuestión salpicada de aristas, matices y recovecos. Contamos con un relativamente nutrido ramillete de resoluciones de distintos ámbitos jurisdiccionales. Su doctrina no siempre ha sido homogénea. Ni es lineal. Se detectan algunas discrepancias y muchos matices diferentes, a veces manifestación de una evolución interpretativa. Incluso en el seno de un mismo órgano se pueden apreciar divergencias y cambios».

Han existido importantes oscilaciones, moviéndose los Tribunales entre posiciones similares a la acogida en la STEDH Bărbulescu II (la citada STS, Social, 26-09-2007, Coruñesa de Etiquetas[24]), e interpretaciones donde, sin embargo, se ha entendido que la mera prohibición absoluta de usos extralaborales ya llevaba implícita una facultad sin límites de control (STS, Social, 06-10-2011, Confecciones Revic y otras[25]; TEDH 2016, Bărbulescu I), o que igualmente tan amplia facultad se desprendería de la mera tipificación de tal prohibición como falta leve (STC 07-11-2013, Alcaliber[26]), pasando, en caso de la Sala Penal del TS por entender, más restrictivamente, que era obligada la exigencia de autorización judicial (STS –Penal – 6.2014, Parques Reunidos[27])

---

[24] Señalaba la Sala que *«lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo para la protección de los derechos humanos»*.

[25] Afirmaba en esta Sentencia el TS que *«en el caso ahora examinado, existía una prohibición absoluta que válidamente impuso el empresario sobre el uso de medios de la empresa (ordenadores, móviles, inernet, etc.) para fines propios, tanto dentro como fuera del horario de trabajo, y no caprichosamente sino entre las sospechas fundadas de que se estaban desobedeciendo las órdenes impartidas al respecto. Y sentada la validez de prohibición tan terminante, que lleva implícita la advertencia sobre la posible instalación de sistemas de control del uso del ordenador, no es posible admitir que surja un derecho del trabajador a que se respete su intimidad en el uso del medio informático puesto a su disposición. Tal entendimiento equivaldría a admitir que el trabajador podría crear, a su voluntad y libre albedrío, un reducto de intimidad, utilizando un medio cuya propiedad no le pertenece y en cuyo uso está sujeto a las instrucciones del empresario de acuerdo con lo dispuesto en el art. 20 ET»*.

[26] Señalaba el TC que, en el supuesto enjuiciado, el Convenio Colectivo aplicable *«…tipificaba como falta leve la "utilización de los medios informáticos propiedad de la empresa (correo electrónico, Intranet, Internet, etc.) para fines distintos de los relacionados con el contenido de la prestación laboral, con la salvedad de lo dispuesto en el artículo 79.2" (…) En tales circunstancias, cabe entender… en el presente supuesto que no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa y que habían quedado registradas en el ordenador de propiedad empresarial. La expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, incluida la adecuación de su prestación a las exigencias de la buena fe [arts. 5 a) y 20.2 y 3 LET] …»*.

[27] Afirmaba la Sala de lo Penal del TS que *«…a nuestro juicio, el texto constitucional es claro y tajante cuando afirma categóricamente que: "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial" (…). No contempla, por tanto, ninguna posibilidad ni supuesto, ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, de la naturaleza del cauce empleado ("correo corporativo"), para excepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia»*.

Por otra parte, también en punto al carácter vulnerador o no de determinados sistemas de registro de los dispositivos digitales, no son coincidentes los órdenes jurisdiccionales social y penal. Por ejemplo, en relación con el registro del ordenador del trabajador o de su USB o de su tablet, facilitados por la empresa, la citada STS (Penal) 23-10-2018 (Rec. 1674/2017) ha señalado que el empleo de la técnica de búsqueda por "palabras ciegas" requiere conocimiento previo del trabajador, pero también su consentimiento, lo que, sin embargo, no exige la jurisprudencia laboral.

b) STEDH 05-09-2017 (Bărbulescu II)

5.3 ¿Cuáles son los antecedentes de hecho de esta importante Sentencia?

En Rumanía, el Sr. Bărbulescu fue despedido disciplinariamente por infringir la normativa interna de la empresa para la que venía prestando servicios, y que prohibía el uso personal de ordenadores, Internet, teléfonos, fax y fotocopiadoras de la compañía. Dicho despido se fundamentó en las transcripciones que la empresa obtuvo a raíz de la monitorización de sus comunicaciones por Internet, y que mostraban que el trabajador intercambiaba mensajes personales con su pareja y familiares a través de la cuenta de Yahoo Messenger creada a instancias de la empresa para comunicarse exclusivamente con clientes.

El Sr. Bărbulescu interpuso demanda alegando la nulidad de la decisión por haberse violado su derecho a la intimidad y al secreto de las comunicaciones, protegidos por la Constitución rumana, el Código Penal y el art. 8.1 del Convenio Europeo de Derechos Humanos (CEDH), en virtud del cual "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia".

Tanto el Tribunal de instancia como el de apelación desestimaron la pretensión del trabajador por considerar que el procedimiento disciplinario había seguido lo estipulado por el Código Laboral y la Directiva 95/46/EC. Contra tal decisión acudió el Sr. Bărbulescu al Tribunal Europeo de Derechos Humanos (TEDH).

5.4 ¿En qué sentido se pronunció el TEDH en su primera Sentencia, Bărbulescu I?

En Sentencia de 12-01-2016, el TEDH desestimó la pretensión del trabajador al entender que no se producía vulneración alguna del art. 8 CEDH.

En concreto, el TEDH consideró **aplicable** al caso el **art. 8 CEDH**, pero concluyó que **no se había vulnerado** el referido precepto puesto que la monitorización llevada a cabo por la empresa fue **limitada y proporcionada**.

Por un lado, el Tribunal expuso que el art. 8 CEDH **no protege cualquier** acción que busque el establecimiento y desarrollo de relaciones interpersonales y que, en cualquier caso, **debe existir una conexión** entre una acción u omisión del **Estado** y la **vida privada** de la persona. Teniendo en cuenta que tanto las comunicaciones como las transcripciones fueron utilizadas como **prueba ante tribunales de lo social rumanos**, dicho precepto **resulta aplicable** en el presente caso. En este sentido, el Tribunal de Estrasburgo reiteró que, aunque la finalidad del referenciado art. 8 es *"**proteger al individuo contra la interferencia arbitraria de las autoridades públicas**, no únicamente obliga al Estado a abstenerse de dicha interferencia: además de su principal tarea negativa, pueden existir **obligaciones positivas** inherentes al efectivo respeto de la vida privada"*.

Por otro lado, respecto de la vulneración de los derechos humanos en juego, el TEDH analizó de manera separada el acceso a las comunicaciones y el uso de las transcripciones como prueba en el juicio:

- **El acceso a las comunicaciones del trabajador** por parte del empresario **es legítimo**. El empresario **actuó bajo la presunción** de que el trabajador **únicamente utilizaba** las cuentas de Yahoo Messenger para **contactar y comunicarse con clientes**, tal y como establecía la política de la empresa y éste había manifestado **previamente**, por lo que el trabajador no podía tener ninguna "*expectativa razonable de privacidad*". Además, **es razonable** que una empresa quiera **verificar** que sus empleados **cumplen con sus obligaciones laborales** durante la jornada laboral.

- Los **órganos judiciales rumanos** ponderaron **correctamente** los derechos e intereses afectados por cuanto **no dieron especial importancia ni a las transcripciones aportadas como prueba, ni al contenido de las comunicaciones**, sino que se limitaron a valorar si la **monitorización** de las comunicaciones en el marco del procedimiento disciplinario era **legal**. De hecho, no se hizo mención de las circunstancias que se comunicaban en los mensajes ni de la identidad de los destinatarios de los mismos.

Por todo lo expuesto, el TEDH concluyó que **no se había producido vulneración** alguna del art. 8 del CEDH.

La sentencia contó, no obstante, con el **voto particular**, **parcialmente disidente**, de uno de los Jueces, en el que se ponía ya de manifiesto que la opinión mayoritaria del TEDH había pasado por alto que no se probó que se hubiera informado suficientemente al empleado de la monitorización de los medios de la empresa –sino solo de la prohibición de uso para fines personales–, y que tampoco se había valorado debidamente la naturaleza sensible de las comunicaciones, que concernían a la salud y vida sexual del empleado. Además, según el Voto Particular, la empresa accedió no solo a la cuenta de Yahoo Messenger creada por el empleado, sino también a su cuenta personal, cuyo nombre ("*Andra te quiere*") no ofrecía dudas acerca de la naturaleza personal de su contenido.

5.5 ¿Cuál es el criterio que, finalmente, aplica el TEDH en su segunda Sentencia, Bărbulescu-II?

En contra del criterio de la Sentencia recurrida, la Gran Sala del TEDH falla en favor del Sr. Bărbulescu. Entiende que el art. 8 CEDH es aplicable, dado que las comunicaciones vía mensajería privada en el lugar de trabajo están protegidas por los conceptos de "vida privada" y "correspondencia".

En este sentido, la Gran Sala establece determinados criterios que los Estados deberían considerar como relevantes cuando sus Tribunales enjuicien casos en los que esté en juego el respeto de la vida privada y la correspondencia en el contexto del empleo. Tales criterios se conocen ya como el **"Test Bărbulescu-II"** y, según este, habrán de tenerse en cuenta los siguientes circunstancias a los efectos de considerar vulnerados los derechos fundamentales del trabajador implicados en el registro de sus dispositivos digitales del trabajo:

(i) Si el empleado ha sido notificado de la posibilidad de que el empleador adopte medidas de control y de aplicación de dichas medidas. Aunque en la práctica los

empleados pueden ser notificados de diversas maneras, dependiendo de las circunstancias concretas de cada caso, la notificación debe ser normalmente clara sobre la naturaleza de la supervisión y debe realizarse antes de su aplicación.

(ii) El alcance de la supervisión por parte del empleador y el grado de intrusión en la privacidad del empleado. A este respecto, debe tenerse en cuenta el nivel de privacidad expuesto, así como las posibles limitaciones de tiempo y espacio y el número de personas que tienen acceso a los resultados.

(iii) Si el empleador ha proporcionado razones legítimas para justificar la supervisión y el alcance de la misma. Cuanto más intrusivo sea el monitoreo, más importante será la justificación que se requiera.

(iv) Si habría sido posible establecer un sistema de seguimiento basado en métodos y medidas menos intrusivos. A este respecto, debería evaluarse, a la luz de las circunstancias particulares de cada caso, si el objetivo perseguido por el empleador podría haberse alcanzado mediante un menor grado de injerencia en la intimidad del empleado.

(v) Las consecuencias de la supervisión para el empleado sometido a ella. Debe tenerse en cuenta, en particular, el uso que haga el empleador de los resultados del seguimiento y si dichos resultados se han utilizado para alcanzar el objetivo declarado de la medida.

(vi) Si el empleado ha recibido las garantías adecuadas, especialmente cuando las operaciones de supervisión del empleador son de naturaleza intrusiva. Estas garantías podrán consistir, entre otras cosas, en informar a los trabajadores afectados o a los representantes del personal sobre la instalación y el alcance de la supervisión, en una declaración de tal medida a un organismo independiente o en la posibilidad de presentar una reclamación.

En aplicación de los criterios expuestos, afirma la sentencia que, en el caso analizado, los Tribunales nacionales no determinaron con claridad si el trabajador había sido informado con carácter previo de las medidas de monitorización y de la naturaleza de las mismas, limitándose a observar que, antes del despido del Sr. Bărbulescu, otra empleada había sido despedida por el uso de internet, el teléfono y la fotocopiadora para fines personales y se había dado traslado de esta información al resto de empleados, por lo que existía una advertencia de que los recursos de la empresa no podían utilizarse para fines no profesionales. Además, para que una advertencia sea válida, tiene que ser previa al inicio de la monitorización, especialmente si ello conllevaba el acceso al contenido de las comunicaciones.

Por otra parte, los tribunales rumanos tampoco tuvieron en cuenta el alcance de la intrusión, a pesar de que el empleador había grabado la totalidad de las comunicaciones. Tampoco se valoró suficientemente qué razones justificaban la monitorización: los tribunales rumanos se refirieron al fin de evitar daños a los sistemas informáticos de la empresa, pero no se probó que el uso realizado por el Sr. Bărbulescu expusiera a la empresa a este tipo de riesgos.

Igualmente, entiende el TEDH que las autoridades rumanas tampoco analizaron adecuadamente si el objetivo perseguido se hubiera podido evitar con una medida menos intrusiva, ni la gravedad de las consecuencias de la monitorización

Finalmente, el TEDH entiende que las autoridades rumanas no determinaron en qué momento exacto del procedimiento disciplinario la empresa accedió a las comunicaciones del trabajador. Aceptar que el contenido de las comunicaciones es accesible en cualquier fase atenta contra el principio de transparencia.

En conclusión, el TEDH considera que los tribunales rumanos no valoraron adecuadamente el equilibrio entre los intereses en juego (vida privada y correspondencia del trabajador vs. derecho de derecho de la empresa a proteger el adecuado desarrollo de su negocio mediante el control de la actividad de sus empleados) por lo que la monitorización y acceso a las comunicaciones personales realizadas con medios de la empresa infringió el derecho a la vida personal y secreto de las comunicaciones del Sr. Bărbulescu garantizado por el art. 8 CEDH.

En definitiva, con esta Sentencia quedan delimitadas las "Reglas del juego":

1. Notificación clara y precisa al trabajador

- De las prohibiciones totales o parciales de uso no profesional del O (DD) → posibilidad de monitorización y su naturaleza
- De los medios de control que utilizará la empresa para tal fin
- De las consecuencias (régimen disciplinario)

2. Necesidad e indispensabilidad de la medida

3. *Como regla general, no cabe suprimir la "privacidad social del trabajador" (ap. 80)*

c) <u>Etapa post Bărbulescu-II</u>

5.6 ¿Se está recibiendo la doctrina Bărbulescu-II en las Sentencias que se están dictando con posterioridad?

Sí. Las Sentencias dictadas tras <u>Bărbulescu-II muestran ya cierta</u> <u>alineación judicial en cuanto a las "reglas del juego", aunque no se ha presentado todavía la ocasión de pronunciarse en todos los aspectos relacionados con esta materia.</u>

<u>Entre los pronunciamientos judiciales que ejemplifican ese alineamiento con la doctrina Bărbulescu-II, podemos destacar los siguientes:</u>

- STEDH 22-02-2018 (Demanda 588/201. Asunto Libert). Se pronuncia acerca del caso de una Entidad pública (empresa nacional de trenes) en la que se permitía el uso privado solo puntualmente y que accede al disco duro del ordenador de un empleado mientras estaba ausente por cumplimiento de una sanción disciplinaria. Tras el descubrimiento accidental de archivos pornográficos, procede a su despido. La Sala admite la validez de la prueba porque, partiendo de que la STEDH <u>Bărbulescu-II</u> subrayó que la proporcionalidad y las garantías procesales contra el carácter arbitrario son esenciales, declara que el derecho positivo francés contiene una regla dirigida a la protección de la privacidad. En concreto, el principio es que, si bien el empleador puede abrir los archivos profesionales almacenados en el disco duro de los ordenadores que pone a disposición de sus empleados para el desempeño de sus funciones, no puede, "excepto riesgo o acontecimiento especial", abrir archivos subrepticiamente identificados como

personales. Únicamente podrá proceder a la apertura de los archivos identificados como personales en presencia de los empleados afectados o después de que hayan sido debidamente informados.

- STS (Social) 08-02-2018 (RCUD. 1121/2015), dictada en el caso Inditex. En el caso enjuiciado, la empresa cuenta con una detallada política de uso estrictamente profesional de los medios de la empresa. Según la Sala, ello conlleva la inexistencia de toda expectativa razonable de privacidad. Dado que se realizó el registro de forma proporcionada al usarse palabras clave y limitado temporalmente, estando el correo corporativo de la empresa alojado en el servidor de la empresa ubicado en sus instalaciones y debiendo aceptar los trabajadores las directrices en Política de Seguridad de la Información del Grupo INDITEX cada vez que acceden al ordenador, la Sentencia considera la prueba así obtenida lícita.

- STS (Penal) 23-10-2018 (Rec. 1674/2017), dictada en el caso Trimarine. La Sala analiza el supuesto de un apoderado/alto cargo de la sociedad, sobre el que se generan sospechas de apropiación indebida de dinero y deslealtad. La Sentencia considera respetada la cadena de custodia del registro del ordenador, pero, conforme a la doctrina Bărbulescu-II, considera la prueba nula, ya que el trabajador no había sido informado previamente.

5.7 Tras Bărbulescu II y la LOPDGDD, ¿qué deberían señalar los Tribunales en relación con los códigos de tolerancia cero en relación con el uso privado de los dispositivos digitales facilitados por la empresa?

Una vez aclarado por el TEDH que *«las instrucciones de una empresa no pueden anular el ejercicio de la privacidad social en el puesto de trabajo»* (STEDH 5-9-2017, Bărbulescu II, parágrafo 80), es claro que las mismas no habilitan a la empresa para acceder total e ilimitadamente al contenido de los dispositivos digitales que utilicen los trabajadores en su prestación laboral.

De acuerdo con este criterio, Sentencias como la STC 170/2013 han quedado desfasadas y no deberían ya tomarse en cuenta para resolver sobre el particular, puesto que no es conforme con la doctrina Barbeluscu-II su aserto según el cual *«la expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales»*.

5.8 Tras Bărbulescu II y la LOPDGDD, ¿qué contenido han de tener los "criterios de utilización" de los dispositivos digitales facilitados por la empresa a los trabajadores?

Ha quedado claro y meridiano, tanto por indicación de la LOPDGDD como del TEDH, que la empresa ha de establecer previamente y comunicar a los trabajadores los criterios de uso de los dispositivos digitales, so pena de vulnerar inevitablemente los derechos fundamentales del trabajador al registrar el uso de los mismo. Pero no concretan ni la Ley ni los Tribunales el contenido de tales normas internas de uso.

Las únicas referencias de la norma al contenido de los criterios de uso de los dispositivos digitales son (i) exigencia de claridad y precisión que impone el art. 87 LOPDGDD respecto

de los usos privados autorizados, y (ii) que se respeten "los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados".

A partir del Test Bărbulescu II y de la doctrina posterior del TS, parece que los criterios de utilización habrán de hacer referencia a los siguientes extremos:

- Determinar prohibiciones de uso (absolutas o parciales)

- Establecer los medios de control que utilizará la empresa para tal fin (software de monitorización o de captura de pantallas, informes periciales informáticos, acceso a contenidos, entre otros).

- Determinar la finalidad y consecuencias de dicho control.

5.9 Tras Bărbulescu II, ¿otorgaría el art. 87 LOPDGDD base de legitimación para registro del ordenador basado en meras sospechas?

No, aunque a partir de esta constatación, las opiniones acerca de la intensidad de los hechos que han de servir de justificación para el registro varían.

Así, opina un sector de la doctrina[28] que, del parágrafo 134 de la STEDH de 05-09-2017 (asunto Bărbulescu-II), se extrae que deberían concurrir **indicios fundados** y no meras sospechas. La Gran Sala alude a que, para justificar con razones legítimas el registro empresarial efectuado, se *«había mencionado la necesidad de evitar una vulneración en los sistemas informáticos de la empresa, el cuestionamiento de la responsabilidad de la empresa en caso de actividad ilegal en el espacio virtual, así como la divulgación de sus secretos comerciales (apartado 28 supra). Sin embargo, a juicio del Tribunal, estos ejemplos solo pueden ser indicaciones teóricas, ya que **no se acusó concretamente** al demandante de exponer a la empresa a ninguno de esos riesgos»*.

Sin embargo, la reciente STEDH 17-10-2019 (Asuntos 1874/13 y 8567/13), dictada por la Sala General (López Ribalda-II), parece rebajar esa exigencia al nivel de "sospecha razonable", al señalar que *«si bien no puede aceptar la afirmación de que, en términos generales, la más mínima sospecha de apropiación indebida o de cualquier otra conducta indebida por parte de los empleados podría justificar la instalación de una vigilancia por vídeo encubierta por parte del empleador, la existencia de una sospecha razonable de que se ha cometido una falta grave de conducta y el alcance de las pérdidas detectadas en el presente caso pueden parecer una justificación de peso. Esto es aún más cierto en una situación en la que el buen funcionamiento de una empresa se ve amenazado no solo por la sospecha de mala conducta de un solo empleado, sino también por la sospecha de una acción concertada por parte de varios empleados, ya que esto crea una atmósfera general de desconfianza en el lugar de trabajo»* (apartado 134)[29].

[28] BAZ RODRÍGUEZ, J. "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático". Trabajo y derecho: nueva revista de actualidad y relaciones laborales, núm. 54, 2019, págs. 49-78.

[29] En este punto, el voto particular formulado por los jueces Gaetano, Yudkivska y Grozev frente a la posición mayoritaria de la Sala General en esta Sentencia, señala que *«…a falta de un requisito de garantías procesales*

5.10 Tras Bărbulescu II y la LOPDGDD, si la empresa respeta en su registro del ordenador las "reglas del juego" (criterios de uso fijados y comunicados internamente) ¿el registro sería ya *per se* válido?

Según hemos podido comprobar, la doctrina judicial interna, en Sentencias no rebatidas aún, ha entendido que a la empresa no se le pueden oponer los derechos del trabajador a su intimidad, al secreto de sus comunicación o a la protección de sus datos personales cuando existe internamente una prohibición absoluta de uso privado de los dispositivos digitales de la empresa, ya sea por haberse establecido así en los criterios de uso internos (STS, Social, 06-10-2011, Confecciones Revic y otras), ya sea por así desprenderse de la tipificación indirecta de tal prohibición como falta leve (STC 07-11-2013, Alcaliber).

Igualmente, del art. 87.3 LOPDGDD se extrae el derecho empresarial de acceso al contenido de los dispositivos digitales respecto de los que haya admitido su uso con fines privados, si se han especificado de modo preciso los usos autorizados y se han establecido garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Sin embargo, de los apartados 120, 132 y 134 de la STEDH Bărbulescu-II se desprende una conclusión contraria, que apela a considerar, en todo caso, con o sin existencia de advertencia previa por parte de la empresa, la proporcionalidad y las garantías procesales frente al carácter arbitrario de los registros de dispositivos digitales.

En definitiva, con base en estos apartados de la STEDH Bărbulescu-II, y a pesar de que las sentencias internas y la LOPDGDD parecen validar registros sin límites de los dispositivos digitales respecto de los que se haya prohibido el uso privado, entendemos que, en todo caso, habrá de superarse también el test de proporcionalidad, tal y como hemos recogido en la respuesta a la pregunta 15 del presente capítulo, a saber:

- Que el registro del dispositivo digital sea idóneo, esto es, eficaz para la consecución del propósito
- Que dicho registro sea necesario, en el sentido de indispensable, porque no no exista otra medida más moderada
- Que el registro haya sido proporcional en sentido estricto, por derivarse del mismo más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en en conflicto

6. PAUTAS DE GESTIÓN EMPRESARIAL

A modo de recapitulación de los distintos argumentos expuestos en los apartados anteriores, es oportuno identificar con claridad las reglas de actuación que deberá observar la empresa que

claras, la existencia de una "sospecha razonable de falta grave de conducta" no es suficiente, ya que puede dar lugar a investigaciones privadas y podría utilizarse como justificación en un número inaceptablemente elevado de casos. Si bien, en principio, el requisito de la "sospecha razonable" es una salvaguardia importante, no es suficiente para proteger el derecho a la intimidad cuando se trata de una vigilancia electrónica de carácter encubierto. En circunstancias como las del presente caso, en las que un empleador utiliza la vigilancia por vídeo encubierta sin avisar previamente a sus empleados, se necesitan salvaguardias procesales adicionales, similares a las exigidas en virtud del Convenio en el uso de la vigilancia secreta en los procesos penales».

pretenda el registro de los dispositivos digitales facilitados a sus trabajadores para el desempeño de su prestación laboral.

6.1 A la vista de la LOPDGDD y de la doctrina judicial europea, ¿cuáles serían las pautas de gestión empresarial claramente establecidas?

En nuestra opinión, las 5 pautas más relevantes para la correcta gestión empresarial del registro de dispositivos digitales que se derivan de la LOPDGDD serían las siguientes:

i. La mera prohibición del uso no profesional de los dispositivos digitales no legitima su libre e incondicionado registro por la empresa

ii. Si la empresa pretende el futuro registro de sus dispositivos digitales puestos a disposición de sus trabajadores, deberá proceder al establecimiento previo de un Código de conducta que determine claramente:

   - Las prohibiciones de uso (absolutas o parciales)

   - Los medios de control que utilizará la empresa para tal fin (software de monitorización o de captura de pantallas, informes periciales informáticos, acceso a contenidos, entre otros).

   - La finalidad y consecuencias disciplinarias

iii. En la confección de dichas reglas de uso, la empresa deberá dar cumplimiento preciso a la intervención de la RLT

iv. La empresa deberá informar a los trabajadores sobre tales criterios de uso de manera integral y continua

v. En todo caso, y a los efectos estrictamente procesales, la empresa deberá guardar rigurosamente la cadena de custodia del dispositivo digital y sus componentes físicos objeto de registro y que contienen la información que se pretender hacer valer como prueba del incumplimiento del trabajador[30]

6.2 En nuestra opinión, ¿cuáles serían otras 6 pautas adicionales de gestión empresarial que consideramos que deberían tenerse también en cuenta por las empresas?

[30] Por ejemplo, la STSJ Madrid (Social) 08-07-2019 (Rec. 416/2019) recuerda que para asegurar la eficacia probatoria de correos electrónicos y otros rastros de información que quedan en el ordenador de un trabajador, es imprescindible que, además de un acceso lícito a dicho dispositivo, esto es, sin haber vulnerado los derechos fundamentales a la intimidad, al secreto de las comunicaciones y al derecho a la protección de datos personales, y de la autenticidad de la información, esto es, que el autor aparente se corresponda con el autor real, es imprescindible que se haya respetado su integridad como medio de prueba, esto es, que quede garantizado que no ha podido existir manipulación, modificación o alteración desde el momento de su extracción o acceso hasta el momento de su aportación al juicio. Por tanto, la eventual búsqueda ciega por palabras que se realice en el ordenador del trabajador, debe ir de la mano de una impecable cadena de custodia. Llama la atención la Sentencia porque no considera cumplido este requisito únicamente con la intervención notarial, ya que el ordenador de la trabajadora *«…no estuvo debidamente custodiado hasta la fecha en el que llegó a la Notaria para su custodia, y por ello a salvo de eventuales manipulaciones externas tanto de carácter cuantitativo como cualitativo»*.

i. Las empresas deberían reflexionar sobre la conveniencia, desde la perspectiva de RRHH, de establecer códigos de "tolerancia cero" en el uso privado de los dispositivos digitales, ya que su existencia no garantiza la ausencia de límites al registro y solo consigue ir contra la realidad de los usos sociales establecidos

ii. Igualmente, las empresas deberían huir de códigos de conducta genéricos o lineales que no tengan en cuenta los diferentes niveles profesionales. Así, por ejemplo, sería razonable establecer dicha tolerancia cero para determinados puestos de trabajo de confianza, cargos directivos, con acceso a información sensible de la empresa, pero podría resultar desproporcionado en el caso de trabajadores sin incidencia productiva ni manejo de datos críticos de la empresa

iii. Las empresas deberán analizar el rol que puede jugar el Convenio Colectivo ex arts. 88 RGPD y 91 LOPDGDD, que puede establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral

iv. Es imprescindible que las empresas incorporen también la validación de sus Códigos de uso de dispositivos digitales por parte del Servicio de Prevención, a los efectos de conectarlos con las obligaciones preventivas

v. También las empresas deberían implementar políticas de formación (y no solo de información) de los trabajadores, mánagers, etc. en esta materia

vi. Finalmente, las empresas deberían dar cumplimiento exacto a lo establecido en el Código, sin caer en la tolerancia de comportamientos que se prohíban, ya que los incumplimientos tolerados pueden dificultar cualquier respuesta sancionadora posterior por parte de la empresa

7. CONCLUSIONES

Con brevedad, y a modo de conclusión, el actual estado de la cuestión hace necesario que los juristas sigamos reflexionado sobre el alcance de la facultad empresarial de registro de los dispositivos digitales facilitados por la empresa a los trabajadores, y ello porque las "reglas del juego", aunque más próximas a despejarse, siguen sin estar completamente claras y unificadas.

Y dicha reflexión debería encaminarse en la siguiente dirección:

- Por un lado, tratando de hacer confluir la gestión jurídica y la gestión de personas en esta materia tan influida por los usos sociales del momento

- Por otro lado, considerando la necesaria reactivación del juicio de proporcionalidad ex art. 18.1 CE

8. BIBLIOGRAFÍA

PRECIADO DOMÈNECH, CH., "Monitorización: GPS, Wearables y especial referencia a los controles biométricos para el registro horario. Aspectos procesales". Capítulo de la presente obra colectiva.

FALGUERA BARÓ, MA. "Nuevas tecnologías y trabajo (y III): perspectiva procesal", Revista Trabajo y derecho: nueva revista de actualidad y relaciones laborales, Nº. 22, 2016, págs. 31-44

BAZ RODRÍGUEZ, J. "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", Trabajo y derecho: nueva revista de actualidad y relaciones laborales, núm. 54, 2019, págs. 49-78.

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", Nueva revista española de derecho del trabajo, núm. 218/2019, págs. 55-86

PEDRAJAS QUILES, A. "Derechos fundamentales de la persona, del trabajador y autonomía privada", en Libro homenaje a Abdón Pedrajas Moreno, coord. por Tomás Sala Franco, 2012, ISBN 978-84-9033-037-1, págs. 403-424.

LUQUE PARRA, M. Y GINÈS I FABRELLAS, A. *Teletrabajo y prevención de riesgos laborales*, CEOE-Fundación para la Prevención de Riesgos Laborales. Madrid, 2016. ISBN 978-84-608-3498-4. Págs. 1 a 119