Anuario IET. Presente y futuro del trabajo | ISSN: 2339-5753

CONTROL TECNOLÓGICO DE LA PRESTACIÓN LABORAL Y DERECHO A LA DESCONEXIÓN: CLAVES TEÓRICAS Y PRÁCTICAS

TECHNOLOGICAL CONTROL OF WORK PERFORMANCE AND RIGHT TO DISCONNECTION: THEORETICAL AND PRACTICAL KEYS

Miguel Ángel Purcalla Bonilla
Universitat Autònoma de Barcelona

MiguelAngel.Purcalla@uab.cat

Resumen

La utilización de la tecnología "digital" en la relación laboral ya no es algo ocasional o esporádico, sino diario y en todo tipo de actividades. La concreción de los límites en el control del uso por los empleados de los instrumentos facilitados por la empresa y el derecho a la desconexión digital de aquellos fuera de su jornada laboral, constituyen, en clave normativa y judicial, el tema abordado en estas páginas, que se cierran con una serie de propuestas concretas para la mejora de la situación actual.

Palabras clave: Videovigilancia; Monitorización; Desconexión digital; Regulación; Límites

Abstract

The use of "digital" technology in the employment relationship is no longer something occasional or sporadic, but daily and in all kinds of activities. The concretion of the limits in the control of the use by the employees of the instruments facilitated by the company, and the right to the digital disconnection of those outside of their working hours, constitute, in normative and judicial key, the topic addressed in these pages, that are closed with a series of concrete proposals for the improvement of the current situation.

Keywords: Video Surveillance; Monitoring; Digital Disconnection; Regulation; Limits

Sumario

1. La dimensión laboral de la profecía orwelliana del controller (*Nineteen Eighty-Four, big brother is watching you*) 96
2. El control tecnológico de la prestación laboral 97
2.1. Uso personal y/o profesional del móvil de empresa 98
2.2. Uso (y control) del ordenador 98
2.3. Vigilancia con cámaras de seguridad 101
2.4. GPS 102
2.5. Control biométrico 104
3. El derecho a la desconexión digital: ¿entelequia, quimera, realidad o desideratum factible? 104
4. Hacia la consolidación de la desconexión digital como derecho laboral: avances reseñables y propuestas de cierre 106
Referencias 109

Referencia normalizada

Purcalla Bonilla, Miguel Ángel (2018): "Control tecnológico de la prestación laboral y derecho a la desconexión: claves teóricas y prácticas". *Anuario IET de Trabajo y Relaciones Laborales*, 5, 95-110. https://doi.org/10.5565/rev/aiet.66

1. La dimensión laboral de la profecía orwelliana del controller (*Nineteen Eighty-Four, big brother is watching you*)

Como es conocido, junto a las técnicas de reproducción de la imagen y el sonido (móviles, cámaras de vigilancia), de la monitorización de ordenadores o de la supervisión de la conexión a internet y del uso del e-mail (programas espía *on line*, programas *accounting* de "control remoto" o "monitorización" off line, tales como ZEIT software, Qactivity, SpyAnywhere, Boss Everyware o NTKlauss –STSJ, País Vasco, Sala Social, 29.9.2015, rec. 1245/2015-), emergen otras como la *geolocalización de los empleados* (sistema de posicionamento global o GPS) o el control biométrico de los trabajadores (huella dactilar, retina-iris, mano, rostro, etc.). El límite para todas ellas es el mismo, en principio: el poder de vigilancia y control del empresario (art. 38 de la Constitución Española –CE-, art. 20 del Estatuto de los Trabajadores –ET-), como legítimo interés en aras a supervisar el correcto cumplimiento de la prestación laboral por el trabajador, debe ponderarse, en cada caso concreto, con los derechos fundamentales y libertades públicas del empleado (dignidad, intimidad, propia imagen, protección de datos personales), lo cual debe ser encauzado a través del *test de proporcionalidad* entre el sacrificio que se leimpone al derecho fundamental restringido y su límite, argumentandola *idoneidad* de la medida, su *necesidad* y el *debido equilibrio* entre el sacrificio sufrido por el derecho fundamental limitado y laventaja que se obtendrá del mismo (Preciado Domènech, 2017).

Con toda claridad se ha escrito que la intimidad del trabajador, el secreto de las comunicaciones, la protección de datos personales, incluso la libertad sindical, llevan años midiendo fuerzas con el uso y control laboral de ordenadores, cámaras de videovigilancia, dispositivos de geolocalización, teléfonos móviles, fichajes informáticos, emisores de radiofrecuencia, etc. (San Martín Mazzuconi, 2017). En caso de colisión de derechos fundamentales o bienes constitucionalmente protegidos, por lo tanto, deben apreciarse "los intereses en presencia, mediante una adecuada ponderación de las circunstancias concurrentes"(SSTCo 99/1994, 6/1995, 106/1996, 136/1996, 204/1997, 98/2000 y 186/2000). De esta doctrina del Tribunal Constitucional se deriva: a) por una parte, que los derechos fundamentales del trabajador "deben adaptarse a los requerimientos de la organización productiva en que se integra" (SSTCo 5/1981,

47/1985, 77/1985 106/1996 y 199/1999); b) por otra parte, que también "las facultades empresariales se encuentran limitadas por los derechos fundamentales del trabajador", que son prevalentes y constituyen un "límite infranqueable" no solo a sus facultades sancionadoras, sino también a las facultades de organización y de gestión del empresario, causales y discrecionales (SSTCo 292/1993, 136/1996, 90/1997, 1/1998, 90/1999, 98/2000, 190/2001, 213/2002, 17/2003 y 49/2003); y c) que:

> Cuando se prueba indiciariamente que una decisión empresarial puede enmascarar una lesión de derechos fundamentales incumbe al empresario acreditar que su decisión obedece a motivos razonables y ajenos a todo propósito atentatorio del derecho de que se trate y que es preciso garantizar en tales supuestos que los derechos fundamentales del trabajador no sean desconocidos por el empresario bajo la cobertura formal del ejercicio por parte de éste de los derechos y facultades reconocidos por las normas laborales" (SSTCo 38/1981, 41/2006, 342/2006 y 125/2007).

En este estado de cosas, en una era como la nuestra, caracterizada por el uso intenso y extenso, global y glocal, de la tecnología como realidad en la vida personal, familiar y profesional (sin que con ello esté formulando un aserto utópico ni mucho menos distópico), se ha activado un debate que no es, precisamente, baladí ni espurio: me refiero a si el trabajador tiene o no derecho a "desconectar tecnológicamente" de su prestación laboral (entendida tal desconexión como el derecho para el trabajador de no tener ningún contacto con herramientas digitales relacionadas con su trabajo durante el tiempo de descanso[Cialti, 2017]) *fuera de su jornada de trabajo diaria* y/o en sus períodos de descanso diario, semanal y/o anual. Como gráficamente se ha señalado, dese hace ya tiempo la vida laboral y la vida privada ya no se concilian, sino que *se mezclan—work and home no longer balance, they blend—*, máxime con el uso de la tecnología en ambas esferas, personal y profesional (Ushakova, 2016), por lo que la concreción de límites se antoja, entiendo, claramente necesaria, en especial en cuanto a si el empleador puede o no controlar tecnológicamente al empleado en ese marco temporal, por decirlo coloquialmente, "extrajornada", y si ello no sólo colisiona con la vida privada del empleado (en orden a evitar lo que se ha denominado, acertadamente, la implantación en la realidad económica de una "empresa panóptica" [Mercader, 2001]) sino, también, con su derecho "laboral" al descanso efectivo, que, como se ha dicho, libera para el trabajador un espacio de autodeterminación, como es el tiempo de no trabajo o el tiempo de vida privada (Molina Navarrete, 2017: 892).

Como se ha expresado con meridiana claridad, el telón de fondo de todo ello es que:

> Los instrumentos tecnológicos operan de consuno en la ejecución del trabajo y en la fiscalización del mismo, y ambos aspectos transitan por espacios insertos en la privacidad e intimidad de las personas-trabajadores (...). Las TIC imponen conductas obligacionales de auto-exploración y hetero-exploración, y en general suponen más trabajo empero fuera del trabajo. Primero diluyen los códigos de espacio y tiempo pues, como dije, normalizan su uso durante las veinticuatro horas a escala planetaria. (...) El tecnoglobalismo dilata expansivamente el esfuerzo cognitivo e intelectual y, al licuarse los códigos de espacio y tiempo, diluye las fórmulas materiales y jurídicas de control digital directivo. Por último, y cerrando la cuadratura del círculo, el funcionalismo tecnológico transforma un objeto físico en objeto social, y a la vez socializa un juego de dependencias socio-emocionales con la utilización compulsiva de los dispositivos móviles" (Alemán Páez, 2017).

¿Cuál es la situación normativa y judicial ante la cuestión apuntada?, ¿existen soluciones a los problemas que suscita?, ¿es necesario un cambio normativo para afrontar mejor los retos que plantea el control empresarial y la desconexión tecnológica de los empleados? Un intento de respuesta (lo que no es precisamente tarea sencilla) a tales interrogantes es el *leitmotiv* que ha guiado la redacción de estas páginas.

2. El control tecnológico de la prestación laboral

Que el teléfono móvil, el ordenador (fijo o portátil), la tablet o el vehículo de empresa (y su rastreo o *teletracking*) puedan ser "fiscalizados", en su utilización por los empleados, por parte de los

empresarios, para comprobar que su uso sea correcto y dentro de los parámetros "autorizados", es algo que puede ser rápidamente comprensible y que, de consuno, provoca lecturas y puntos de vista muy diversos. No es demasiado novedoso indicar que existe jurisprudencia y doctrina judicial que ha abordado la cuestión desde hace años. Lo primero que debe tenerse en cuenta es que el control empresarial de la prestación de servicios por cuenta ajena, debe ser *proporcional* y debe respetar la intimidad y la dignidad de los empleados (arts. 4.2.e y 20.3 del Estatuto de los Trabajadores —ET—). En clave de teletrabajo o, sencillamente, del *uso de las herramientas informáticas*, la Directiva 90/270, de 29 de mayo (sobre pantallas de visualización de datos —PVD—), refiere en su Anexo que no deberá utilizarse ningún dispositivo cuantitativo o cualitativo de control sin que los trabajadores hayan sido informados.Así las cosas y señalado dicho punto de partida, no está de más recordar de dónde venimos (*once upon a time...*) en este tema para poder plantear hacia dónde vamos (*where are we going?*), mediante una serie de criterios-guía que, espero, resulten útiles al lector.

2.1. Uso personal y/o profesional del móvil de empresa

Respecto al *uso personal y/o profesional del móvil "de empresa",* la regla general es que con tarifa plana y sin prohibición expresa de uso particular, existe una tolerancia implícita y no es posible imponer sanción alguna contra el empleado (STSJ Madrid 27.6.2007, rec.2233/2007 y STSJ La Rioja 12.3.2009, rec.108/2009). Como excepción, pueden implantarse prohibiciones de uso privado/corporativo (razones de seguridad, personal de circulación de ADIF, evitar distracciones —SANac 17.4.2017, proced. 56/2017—)en el trabajo. En consecuencia, sería un despido "procedente" (ergo, correcto, si bien cabe, en función del caso concreto, sanción disciplinaria menor —STSJ Castilla y León 22.12.2017, rec. 1665/2017—)el que se adopta contra un empleado por uso abusivo del teléfono de empresa, facilitado sólo para llamadas de voz (Nokia), con fines personales (no siendo posible más que un uso privado, ocasional y excepcional en caso de emergencias personales/familiares —pues tales forman parte de su vida privada, SSTEDH 25.6.1997, *Halford vs. Reino Unido*—) y con uso no autorizado de internet móvil con costes excesivos (STSJ Canarias 20.12.2013, rec. 435/2013, o en casos similares, STSJ Cataluña 30.9.2009, rec. 3953/2009 y STSJ Madrid 18.3.2013, rec. 5131/2012). Por lo demás, sólo es sancionable el uso "indebido" personal no autorizado si se produce durante el tiempo de trabajo, pero no si tal uso no se produce de modo probado en tiempo de trabajo (o si no se cuestiona el uso personal no excesivo fuera del horario de trabajo, al no estar prohibido explícitamente), pues en tal caso el despido sería incorrecto, ergo "improcedente" (STSJ Cataluña17.10.2016, Rº 4132/2016).

2.2. Uso (y control) del ordenador

Respecto al *uso del ordenador* (programas, aplicaciones, e-mail), la casuística, hasta la fecha, es muy considerable, lo que expresa de modo elocuente el interés del tema. En un afán de síntesis y a modo de explicación práctica de los principales *leading cases*, debe indicarse que los tribunales señalaron que al registro del ordenador (como al de un vehículo de empresa) no le resultan de aplicación las garantías del art. 18 ET, pues no tienen la consideración de efectos personales de un empleado, como por ejemplo una taquilla en el vestuario (SSTS 26.9.2007, u.d. 966/2006—que admitió el uso privado "moderado" del ordenador y señaló que debe informarse a los empleados sobre las políticas de "uso prohibido", loque recoge, por ejemplo, el art. 8 del CC general de la Industria Química, en concordancia con las SSTEDH 3.4.2007, asunto *Copland vs. Reino Unido* y 1.7.2008, asunto *Liberty vs. Reino Unido*— y 8.3.2011, u.d. 1826/2010 y con la STSJ Cataluña 7.11.2014, rec. 4585/2014).

Como indica la STSJ Madrid 30.10.2009 (rec. 4050/2009),

> No es lo mismo registrar la taquilla o el bolso de un trabajador que su ordenador porque, aunque en ambos casos pueden encontrarse elementos personales, la finalidad del continente es distinta. Sólo será posible efectuar registros sobre elementos personales de los trabajadores cuando éstos sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo y en ellos habrá de respetarse al máximo la dignidad e intimi-

 ISSN: 2339-5753

> dad del trabajador. Además, habrá de efectuarse en presencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible. En estos registros el empresario actúa, de forma exorbitante y excepcional, fuera del marco contractual de los poderes que le concede el art. 20 ET y, en realidad, desempeña una función de policía privada o de policía empresarial que la ley vincula a la defensa de su patrimonio o del patrimonio de otros trabajadores de la empresa. Por el contrario, cuando se trata de medidas de control sobre los medios informáticos puestos a disposición de los trabajadores forman parte del poder de dirección ordinario: el ordenador es un instrumento de producción del que es titular el empresario y éste tiene, por tanto, 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, lo que no sucede en los supuestos del art. 18 ET , pues incluso respecto a la taquilla, que es un bien mueble del empresario, hay una cesión de uso a favor del trabajador que delimita una utilización por éste que, aunque vinculada causalmente al contrato de trabajo, queda al margen de su ejecución y de los poderes empresariales del art. 20 ET para entrar dentro de la esfera personal del trabajador.

En Francia, la *Cour de Cassation*(5.7.2017) ha señalado que no es motivo de despido la negativa del trabajador a facilitar un USB para que el empleador consulte su contenido, pues contiene archivos no sólo profesionales sino personales. Los archivos "profesionales" del USB sí pueden ser consultados, pero en presencia del trabajador (Cour de Cassation 21.10.2009, 4.7.2012 y 12.2.2013).

Profundizando en cuanto al *uso del ordenador de la empresa y su control*, no se vulnera la intimidad ni el secreto de las comunicaciones (ni su dignidad) si no se accede a información personal o familiar de un trabajador, practicando al efecto una prueba pericial informática con registro del ordenador en presencia del trabajador y con una finalidad evidente, como prueba *necesaria, idónea y proporcionada* para obtener la confirmación de los indicios o sospechas, por ejemplo, de competencia desleal de un empleado (STS 26.9.2007, u.d. 966/2006). En esta línea, en Francia se ha aceptado la corrección de un despido disciplinario por uso indebido y no profesional, no autorizado, del e-mail "profesional", pudiendo ser consultado su contenido en presencia del empleador (Cour de Cassation, 16.5.2007 y 18.10.2011), pero *no se puede consultar elcontenido de un e-mail "personal"*(Cour de Cassation,16.5.2013) porque *debe ser respetado el secreto de la correspondencia* (Cour de Cassation,26.1.2016).

En concreto, la técnica de la *búsqueda ciega por palabras clave* (programa *Encase Forensic*—a modo de ejemplo, STSJ Andalucía-Sevilla 17.12.2007, rec. 1050/2007—) entre los rastros de información que quedan en el ordenador de un trabajador (en el disco duro, específicamente) facilitado por la empresa, a propósito de las comunicaciones realizadas por éste con terceros que guarden relación con los indicios y sospechas de competencia desleal, debe ir de la mano de una *impecable cadena de custodia* (precinto y copia del disco duro depositado notarialmente, pericial informática por empresa independiente, información y conocimiento en todo momento del empleado sobre los motivos de tal proceder y proceso seguido al respecto), sin que dicha prueba constituyauna vulneración del secreto de comunicaciones (contenido de la misma e identidad subjetiva de los interlocutores —SSTCo 114/1984, 70/2002 y 56/2003—) del empleado ni de su derecho de intimidad, si el perito informático no interfiere ningún proceso de comunicación ajena, sino que se limita a llevar a cabo una *lectura ciega a través de una herramienta informática que no conlleva la lectura de toda la información sino sólo para detectar lo relevante para la empresa*, mediante la utilización de palabras clave (*método poco invasivo*—copia del disco durooriginal, que se precinta notarialmente y se le da un número hash, como funciones de resumen que consisten en algoritmos que crean, a partir de una entrada, ya sea un texto, una contraseña o un archivo, una salida alfanumérica de longitud normalmente fija—y cadena ulterior de custodia, pericial informática sobre palabras ciegas y análisis heurístico) que sólo permiten rescatar lo que interesa (STS 8.2.2018, u.d. 1121/2015); esto es, "supone la posibilidad de discriminar lo que se busca e interesa, que guarda relación con la empresa y con los posibles actos de competencia desleal, sin que afloren ni tengan acceso terceros a otra informa-

ción más personal" (Auto de la Audiencia Provincial de Barcelona 9.7.2010, rec. apelación 218/2010, AC 2010/1635).

Es más, aunque la prueba informática obtuviera un "hallazgo casual", la STS, Sala Penal, de 4.12.2015 (rec. 10477/2015) afirma la validez de la información obtenida en determinadas circunstancias en el examen de un ordenador,aun cuando la obtención de aquélla no fuera el objeto de ese examen realizado, de modo que, obtenidos incluso tales hallazgos, se puede utilizar como medida disciplinaria en función de la gravedad del ilícito cometido (STSJ Madrid 15.7.2016, rec. 399/2016).

No existe vulneración de expectativa razonable alguna de privacidad (SSTEDH 25.6.1997, asunto *Halfor,* 3.4.2007, asunto *Copland* y 1.7.2008, asunto *Liberty*) cuando *el control empresarialde un ordenador no ha resultado ni excesivo ni desproporcionado* para la satisfacción de los intereses empresariales frente a la competencia desleal, siendo la prueba pericial informática practicada *susceptible de conseguir el objetivo propuesto —juicio de idoneidad—, 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 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*—(SSTCo 14/2003, 89/2006, 12/2012, 96/2012 y 170/2013, SSTEDH 12.1.2016, asunto *Barbulescu* I y 5.9.2017, asunto *Barbulescu* II). De este parecer es la más reciente STEDH de 22.2.2018, asunto *Libert vs. Francia*, que ha señalado la corrección del legítimo interés del empleador en asegurar el buen funcionamiento de su empresa y el uso correcto de los equipos informáticos puestos a disposición de los empleados para el desempeño de sus funciones, aplicando medidas que le permitan verificar que sus empleados cumplen con sus deberes profesionales de manera adecuada y con la celeridad requerida, cuando detectaen un registro informático de ordenadores *archivos no identificados claramente como privados* de acuerdo con el manual de usuario de la empresa (que permitía, en ausencia del empleado, abrir los archivos marcados como profesionales y no como privados) y atendido su contenido (imágenes y películas de carácter pornográfico y/o humorístico), validando el despido de dicho empleado.

) Seguimos en el tema del control del ordenador (y acabamos al respecto con este apartado), ahora ya con la lectura más actualizada de la jurisprudencia de interés al respecto. Si en una primera aproximación, la STEDH de 12.1.2016 (asunto Barbulescu-I) indicó que "una empresa puede controlar los mensajes de sus trabajadores en un servicio de mensajería instantánea profesional a través de Internet, siempre que previamente hubiera prohibido de modo expreso el uso de los medios de comunicación de la empresa (Yahoo Messenger) para fines personales" (en sintonía con la potestad disciplinaria de las empresas cuando el trabajador incumple la prohibición de uso personal de un ordenador —SSTCo 241/2012 y 170/2013, STSJ Cataluña 13.6.2016, rec. 2131/2016, STSJ Madrid 26.1.2015, rec. 679/2014—), con posterioridad se debe tener en cuenta lo siguiente: a) que las SSTCo 173/2011 y 142/2012 indicaron que el e-mail tiene la protección del derecho a la intimidad y al secreto de las comunicaciones en cuanto a su contenido; b)la más reciente STEDH 5.9.2017 (asunto Barbulescu-II), *revoca* el criterio de la STEDH 12.1.2016 (Barbulescu-I), indicando 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.

Añadiendo la consideración de que *la mensajería electrónica enviada desde una cuenta profesional debe considerarse correspondencia* (art. 8 CEDH); sin embargo, el artículo 8 CEDH no menciona específicamente la protección de datos de carácter personal, que en cambio aparece recogida como un derecho autónomo en el artículo 18.4 de la Constitución española y en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea (tampoco puede olvidarse que conforme al art. 6.2 del Reglamento General de Protección de Datos —que establece que será lícito el tratamiento cuando *sea necesario para la ejecución de un contrato en el que el interesado es parte o para*

 ISSN: 2339-5753

la aplicación a petición de este de medidas precontractuales—, de suerte que, como se ha entendido con acierto, la monitorización del ordenador, del uso de internet, del uso del teléfono o la videovigilancia del trabajador entrarían dentro de ese concepto [Todolí, 2018]).

Lo más relevante, empero, de la sentencia Barbulescu-2 es que supone que:

> Los jueces nacionales deben examinar si el trabajador ha sido informado previamente de la posibilidad de que el empresario aplique medidas de control de las comunicaciones,exigiendo que el trabajador tenga información previa y clara sobre los sistemas de vigilancia—principio de transparencia—, además de exigir un control intenso de proporcionalidad en el caso del acceso al contenido de los mensajes(García Vitoria, 2018).

2.3. Vigilancia con cámaras de seguridad

Con relación a la *vigilancia con cámaras de seguridad*, es evidente que debe tratarse de una medida proporcional, idónea, necesaria y razonable (por ejemplo, por razones de seguridad —expresión amplia que incluye la vigilancia de actos ilícitos de los empleados y de terceros y la seguridad del centro de trabajo—), debiendo existir información con "distintivos" de zona videovigilada en los centros de trabajo (Instrucción AEPD 1/2006, STCo 29/2013, SSTS 31.1.2017, u.d. 3331/2015 y 2.2.2017, u.d. 554/2016).La prohibición de videovigilancia empresarial es *especialmente contundente*cuando las cámaras se instalan en lugares de uso personal (como servicios —salvo entrada/salida—, vestuarios —salvo entrada/salida—, comedores, zonas de descanso —salvo cámara sin imagen de sonido y por razones de seguridad y/o control de accesos—, etc.), considerados "lugares reservados".

La implantación de videocámaras para "monitorizar" una actividad, debe estar justificada y debe ser proporcionada a la finalidad prevista (SSTSJ Andalucía-Sevilla 22.3.2017, rec. 1461/2016 y 11.10.2017, rec. 3345/2016, STSJ Comunidad Valenciana 13.10.2017, rec. 347/2017, STSJ Cataluña 5.10.2017, rec. 2833/2017, STSJ Andalucía-Málaga 17.1.2018, rec. 1878/2017), pues en caso contrario se conculcaría la intimidad de los empleados (STEDH 28.11.2017, asunto *Antovic y Mirkovic*, art. 8 CEDH, a propósito de cámaras en las aulas de un instituto universitario de matemáticas en Montenegro, que grababan de modo permanente las clases de dos profesores).

Ahora bien, deben tener conocimiento los trabajadores de la implantación en la empresa de tales cámaras (regla general), salvo que las mismas, como excepción, tengan como finalidad acreditada la de servir como medio para acreditar incumplimientos de concretos trabajadores, no pudiendo ser grabada toda la plantilla y debiendo tener tal grabación "sorpresiva" u "oculta" un *marco temporal acotado y una sospecha o indicio fundado* (STEDH 9.1.2018, asunto *López Ribalda*, en un caso en el que por las sospechas de la dirección de la empresa —supermercado—, provocadas por la falta de correspondencia entre la facturación y el inventario de los productos, se instaló un sistema de cámaras, algunas visibles y otras ocultas que enfocaban directamente a las cajas y se informó a los trabajadores de la existencia solo de las cámaras visibles).

En conclusión: si una empresa quiere instalar cámaras de videovigilancia, *debe informar* a sus trabajadores de ello (si la cámara se instala de modo permanente y/o prolongado—SSTSJ Cataluña 19.2.2018, rec. 6637/2017 y 16.3.2018, rec. 154/2018—) y de la existencia de un fichero con datos de carácter personal (la imagen lo es), así como de que las grabaciones podrán ser utilizadas para justificar un incumplimiento (transparencia informativa); si la cámara sólo se instala durante pocos días (los necesarios para confirmar la sospecha previa) y sólo graba alrededor del puesto de trabajo (sin grabar a nadie más ni en lugares controvertidos), puede defenderse la proporcionalidad, idoneidad y necesidad de la medida (López Cumbre, 2018). Ligado a ello, es claro que las empresas deben cumplir con el criterio de la STCo 39/2016, del art. 5 LOPD y del art. 3 de la Instrucción 1/2006 AEPD, en el sentido de ubicar distintivos informativos en lugar visible (espacios abiertos o cerrados) e información sobre el tratamiento de datos obtenidos con las grabaciones, pues en caso contrario la prueba de grabación aportada sería ilícita y el despido basado exclusivamente en la misma sería nulo (STSJ Cataluña 22.3.2018, rec. 255/2018, STSJ País Vasco

7.2.2018, rec. 226/2018, STSJ Castilla-La Mancha 12.1.2018, rec. 1416/2017).

De esta guisa, la utilización empresarial de cámaras de videovigilancia "sin sospechas previas sobre una posible conducta irregular del trabajador, decide controlar aleatoriamente (la empresa) su forma de prestar servicios mediante cámaras que instala, sin informarle sobre esa posibilidad (falta de transparencia informativa), para después despedirle, en atención precisamente, a esas imágenes "captadas por la cámara", siendo tal prueba, así obtenida, ilícita (STS 13.5.2014, u.d. 1683/2013, STSJ Madrid 23.4.2018, rec. 74/2018). El despido, por lo tanto, sería nulo por vulneración del derecho a la intimidad cuando se instalan cámaras de vigilancia y micrófonos en el vehículo de un empleado, sin una mínima informaciónprevia al respecto, máxime si incluyen, además de la grabación visual, las conversaciones mantenidas por el trabajador (STSJ Castilla-León 11.4.2018, rec. 407/218, con cita de la STCo 98/2000 —asunto *Casino La Toja*— y la indicación de que "aunque una video grabación limitada en el tiempo para detectar las irregularidades hubiera podido ser válida hipotéticamente, no lo es por faltar la más mínima información sobre la instalación de las cámaras de vigilancia en el recinto del centro de trabajo y por incluir, además, la grabación de las conversaciones mantenidas por el trabajador").

2.4. GPS

En relación con la *implementación de GPS(Global Positioning System)* en vehículos (rastreo acoplado a una red digital de comunicaciones móviles GSM —*Global System for Mobile Communications*—) para controlar su uso (rutas, consumos, entregas, paradas/arranque, visitas a clientes), e incluso respecto al GPS en tablets y/o teléfonos móviles facilitados por la empresa, para comprobar el cumplimiento de las obligaciones laborales de sus empleados, muchas son las reflexiones que cabe efectuar, que vamos a tratar de sintetizar al máximo.

En primer lugar, GPS y GSM *afectan a una de las manifestaciones del derecho a la intimidad, en concreto, el derecho a que los demás no sepan dónde se está en cada momento*; es decir, el derecho a no estar "permanentemente" localizado por medios electrónicos colocados en el vehículo o en el móvil o en el ordenador o en la tablet. Cuestión distinta es que el GPS implantado en una tablet y con conocimiento del empleado, constituye instrumento válido para constatar incumplimientos laborales, por ejemplo, de un comercial (STSJ Asturias 3.10.2017, rec. 1908/2017).

En segundo lugar, existe una diversidad de pronunciamientos en derredor de la cuestión relativa a si el trabajador debe conocer o no la implantación de sistemas de rastreo GPS en su vehículo o en su móvil: favorables a dicho conocimiento se muestran, que tildan de ilícita la prueba obtenida vía GPS si el empleado desconocía su existencia y si además, se control de ese modo el lugar exacto en el que está el empleado, incluso fuera de su jornada de trabajo (STSJ Castilla-La Mancha 10.6.2014, rec. 1162/2013, STSJ País Vasco 2.7.2007, rec. 1175/2007, en asuntos de rastreo de móvil profesional, y SSTSJ Madrid 21.3.2014, rec. 1952/13, 29.9.2014, rec. 1993/13 y 11.9.2017, rec. 589/2017, en asuntos sobre GPS en vehículo de empresa sin información previa al empleado), criterio que, jurídicamente, me parece el más acertado, de suerte que la información previa de la instalación de GPS es lo más recomendable, en sintonía con el Dictamen Grupo PD 5/2005 de la UE (STSJ Comunidad Valenciana 2.5.2017, rec. 3689/2016), con el art. 5.2 LOPD y con la resolución AEPD de 9.2.2016, expediente nº E/03038/2015(STSJ Castilla-La Mancha 28.4.2015, rec. 134/2015); mientras otros pronunciamientos refieren que no se precisa el conocimiento (ni mucho menos el consentimiento) del empleado sobre aquella implantación, pues la empresa puede instalarlo para comprobar que un comercial realice las rutas correctas (SSTSJ Cataluña 5.3.2012, rec. 5194/2011, STSJ Andalucía-Granada 15.7.2015, rec. 1264/2015, STSJ Galicia 26.4.2017, rec. 510/2017).

En conclusión: entiendo que información *sí debe darse al empleado* (sobre la implantación del GPS y la finalidad que con la misma se persigue), *no siendo necesario un consentimiento específico del trabajador al tratamiento de datos* (en este sentido, STSJ Castilla-La Mancha 31.3.2015, rec. 19/2015), de modo que, si ha sido informado y pese a ello incumple con su ruta comercial, el empleado puede ser objeto de sanción disciplinaria, despido disciplinario incluido (STSJ Andalu-

cía-Sevilla 19.7.2017, rec. 2776/2016, STSJ Andalucía-Granada 18.9.2017, rec. 770/2017, STSJ Castilla-La Mancha 25.1.2018, rec. 1662/2017). ¿Dónde está el límite? Sencillo: cuando finaliza la jornada laboral o acaba el tiempo de trabajo, las facultades empresariales de control vía GPS desaparecen (por lo que el sistema de control debe dejar de estar operativo) y el contrato de trabajo deja de constituir el vínculo entre las partes que ampara el poder de la empresa para imponer las medidas implantadas de captación y tratamiento de datos, de suerte que, a partir de ese momento, es imprescindible el consentimiento de los trabajadores para mantener en funcionamiento los dispositivos GPS y para el análisis automatizado de los datos personales conseguidos por ese medio (STSJ Asturias 27.12.2017, rec. 2241/2017).

A modo de cierre, dos pinceladadas de derecho comparado. Así, a diferencia del caso de España (donde la "anomia es la norma", valga el juego de palabras), en Italia sí existe normativa que regula la implantación de GPS en vehículos o dispositivos móviles de los empleados facilitados por su empleador. En concreto, el art. 4 del *Statuto dei Lavoratori* refiere que la instalación de GPS de control requiere del previo acuerdo con los representantes sindicales o, a falta de éstos, de previa autorización de la Inspección de Trabajo, si se trata de medidas adicionales de seguridad en el trabajo o de razones organizativas/productivas (regla general). Como excepción, si son GPS en coches, furgonetas, autocares o camiones de la empresa, sólo se exige previa información al empleado de su implantación si es necesario llevar GPS por ley o reglamento (por ejemplo, transporte de pasajeros, de productos inflamables/explosivos o de caudales, servicios de emergencia o de reparación "móvil", transporte de personas en embarcación de línea "no regular" en Venecia —ej., Burchiello o Vaporetto—), de modo que el rastreo GPS previamente informado permite el despido disciplinario por absentismo no justificado (Cassazione Lavoro nº 20440, de 12.10.2015); mientras sí se puede instalar GPS de "control"en móviles o tablets de empresa pero con previa información al trabajador. Como ha señalado el *Provvedimento* (equivalente a una Orden Ministerial en España) nº 247, de 24 de mayo de 2017, no cabe geolocalización permanente de los empleados (derecho a "desconectar" fuera del horario laboral, salvo profesiones singulares —tiempo de disponibilidad, tiempo de localización, etc—), cumpliendo así el legislador italiano con la sentencia de la Corte di Cassazione nº 19922, de 5.10.2016.

En el caso de Francia, la sentencia de la *Cour de Cassation Sociale* de fecha 17.12.2014 ha fijado claramente el criterio de que el trabajador ha de poder desconectar el GPS en su tiempo de"pausa", de modo que no se le puede despedir si rechaza la instalación en el vehículo de empresa que conduce de un sistema de geolocalización. De su lado, la sentencia de la *Cour de Cassation Sociale* de fecha 3.11.2011 ha indicado que se precisa información previa a los empleados sobre la finalidad de la implantación del GPS, así como sobre el tiempo de conservación y tipo de datos obtenidos, derecho de acceso y rectificación, además de que deba tal implantación ser comunicada a la CNIL (*Commission nationale de l'informatique et des libertés*), equivalente en Francia a la AEPD**.** Cabe añadir dos precisiones (a modo de "buena práctica" que debiera ser observada en España como guía en este tema): como ha señalado la *Cour d'Appel*de Bordeaux el 27.11.2012, el GPS instalado en el vehículo profesional de un empleado, debe poderse desconectar por éste mientras realiza funciones sindicales; mientras la *Délibération n° 2006-066, du 16 mars* (*Recommandation relative à la mise en oeuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public*, de la *Commission nationale de l'informatique et des libertés*), indica que sólo es admisible la implantación de GPS en los vehículos por razones de seguridad y salud de los trabajadores (transporte de mercancías, trabajo en condiciones de aislamiento, transporte de dinero, transporte de personas —escolar—, limpieza de carreteras y arcenes, patrullas policiales, máquinas quitanieves, control de la velocidad empleada) o por necesidad de localización por el tipo de prestación (servicio de urgencias, taxis, talleres móviles de reparaciones, etc.), pero el GPS no puede implantarse para controlar a empleados con libertad para fijar sus rutas (visitadores médicos, vendedores ambulantes, comerciales/representantes).

2.5. Control biométrico

Respecto al *control biométrico* de los empleados mediante instrumentos tecnológicos, debe señalarse que la "versión digital" de una huella dactilar «no expresa ningún aspecto concreto de la personalidad»; que los datos biométricos no tienen mayor trascendencia que los «datos relativos a un número de identificación personal», o de una ficha personal; que los empleadores pueden emplear tecnologías de reconocimiento biométrico en el control horario, al no haber «norma que prohíba el recurso a la tecnología escogida para realizar el control del cumplimiento del horario de trabajo» (STS 2.7.2007, Sala Contenciosa, a propósito de resolución del Gobierno de Cantabria que implantaba un sistema de control horario con lectura biométrica de la mano); así como que la lectura biométrica de la mano mediante un escáner que utiliza rayos infrarrojos y que es inocuo para la salud no puede considerarse lesivo para el derecho a la integridad física y moral (STSJ Murcia 25.1.2010, rec. 1071/2009).

No es por ello inusual encontrar pronunciamientos que indican que la captación por un sistema electrónico de determinados parámetros biométricos de la huella digital, mediante tratamiento informático, con el fin de controlar su acceso a las instalaciones de la misma, no reviste caracteres de intromisión ilegítima en la esfera de la intimidad, tanto por la parte del cuerpo utilizada, como por las condiciones en que se usa, pues no existe constancia de la utilización de tales datos para fines diversos y porque con ocasión de la lectura de la huella digital no se puede ver la imagen de la huella ni puede ser captada por terceros, quedando todos los datos del sistema guardados en los ordenadores de la empresa a efectos de su custodia: así, STSJ Cataluña, Sala Social, 28.11.2016, rec. 3933/2016, a propósito de marcaje biométrico horario —huella digital— en el SOC, o las SSTSJ Canarias, Sala Contenciosa, de 18.4.2012, rec. 357/2009, 31.10.2012, rec. 386/2007, 9.11.2012, rec. 356/2009 y 3.6.2013, rec. 391/2009, que señalan que el mecanismo de control horario —imagen biométrica de la mano— no vulnera la intimidad e integridad personal protegida constitucionalmente, pues se reduce a ser un *algoritmo digitalizado de la imagen de la mano*. Como indica la STSJ Canarias, Sala Social, 29.5.2012 (rec. 398/2012):

> En realidad, la captación de imágenes o registros de distintas partes del cuerpo humano a efectos de identificación no es desconocida. Así, no se considera lesiva la fotografía del rostro o del cuerpo entero, se admite la toma de huellas digitales o del pie, el registro del iris o de la voz y hasta del mismo ADN en determinados supuestos.

Cuestión distinta es la relativa a que la empresa debe informar a los trabajadores de la existencia de registro de datos, derechos de rectificación y cancelación, etc. (art. 5 LOPD), pues en caso contrario la AEPD puede imponer sanciones (por ejemplo, expediente 617/2010, sanción impuesta por la AEPD a la empresa EULEN, confirmada por el Tribunal Supremo, Sala Contenciosa, sentencia de 21.6.2013, rec. 483/2011).

3. El derecho a la desconexión digital: ¿entelequia, quimera, realidad o desideratum factible?

El denominado "derecho a la desconexión" forma parte de la candente actualidad de los temas laborales que están siendo objeto de análisis por la doctrina científica, pero no sólo por ella. Prueba de lo que se dice es que el boletín de la Comisión Consultiva Nacional de Convenios Colectivos (2017) recoge un comentario en el que refiere que el desarrollo de las tecnologías puede tener una lectura positiva—uso correcto— (mayor flexibilidad en el desempeño de las funciones en clave de conciliación de la vida laboral, familiar y personal) y una lectura negativa (uso incorrecto y exagerado) en tanto que la posibilidad de comunicación constante que ofrece la tecnología puede desembocar en un control exhaustivo del trabajador, no permitiendo la "desconexión" de la vida laboral una vez realizada la jornada de trabajo diaria o semanal.

Para algunos autores, el derecho a la desconexión no precisa de positivización alguna, pues no deja de ser una explicitación de un derecho al descanso que ya tienen los trabajadores reconocido por Ley y convenio colectivo, de modo que:

> El pretendido nuevo (o estatus naciente) derecho de desconexión laboral no existe co-

 ISSN: 2339-5753

> mo tal, autónomo y diferenciado, sino que es, en realidad, una concreción del contenido del viejo —o clásico— derecho, actualizado bajo el impuso adaptativo de las nuevas necesidades creadas por la tecnología digital —art. 3 CC—, al descanso, hoy derecho social fundamental comunitario (Molina Navarrete, 2017: 916).

Mientras otros autores defienden, como importante avance, su positivización (Alemán Páez, 2017).Con mayor dureza si cabe y en sentido negativo hacia el reconocimiento del derecho en cuestión, se ha señalado que, si la desconexión digital supone que:

> Los trabajadores puedan apagar el móvil terminado su horario de trabajo, el derecho a no contestar llamadas o mensajes o emails de trabajo fuera del horario de trabajo ya existe. La legislación reconoce unos límites a la jornada diaria, semanal con descansos mínimos obligatorios entre jornadas. Pero de hecho, ni siquiera parece necesario recurrir a los descansos legales para justificar poder dejar sin responder una llamada. En realidad, es suficiente con entender que fuera del horario de trabajo, el trabajador no tiene obligaciones laborales [e] impugnar las sanciones recibidas en caso de negativa a recibir "trabajo" fuera de la jornada (Todolí, 2017).

Por ello y terciando en ese debate, entiendo que no encierra ni obedece ni una quimera ni una entelequia, como tampoco a una realidad ya consolidada y acrisolada (más bien lo contrario), sino a un *desideratum factible y realizable*. Me explico: en su día, Jeremy Bentham aludía al "sentimiento de omnisciencia invisible" en el contexto de una propuesta de arquitectura carcelaria "panóptica" (ámbito penal y penitenciario), lo que, traducido en clave laboral, significaría que *el empleado se sabe observado, pero no sabe cuándo*, siendo palmario que debe evitarse a toda costa esa percepción en los empleados, que generaría, sin duda, riesgos psicosociales multivarios (tecnoestrés, *burnout*, ansiedad, tecno-adicción, tecnofobia), como indican, entre otros, Talens Visconti (2018) y Moreno González-Aller (2018). Noticias como la relativa a la empresa Three Square Market (32Market), en EEUU (Wisconsin), a propósito de un programa piloto de implantación (colabora la empresa sueca BioHax) a trabajadores "voluntarios" de microchips inalámbricos de identificación por radiofrecuencia (tamaño de un grano de arroz) a los trabajadores, en la mano, entre el pulgar y el índice (para el acceso al trabajo, hacer fotocopias, acceder a ordenadores, tablets, smartphones o iphones, almacenar datos médicos y profesionales, etc.), no constituyen una perspectiva demasiado halagüeña y, por ende, entiendo que vulnera el derecho a la intimidad porque el *chip* en cuestión es "pequeño pero matón", porquelleva GPS incorporado 24 horas al día y 365 días al año, sin que pueda "desactivarse" salvo que se extraiga de la mano del empleado.

La doctrina científica ha expuesto otros ejemplos, señalando que la empresa de videovigilancia Citywatcher.com, de Cincinnati, Ohio (EEUU), empezó a utilizar en 1996 los "chips" para controlar el acceso de sus empleados a las zonas de seguridad restringidas de la compañía; mientras, más recientemente, la empresa belga Newfusion, especializada en marketing digital, ha implantado a varios empleados un chip bajo la piel que funciona como una llave de identificación para abrir puertas y "Según la compañía, el chip no permite localizar al trabajador ni tampoco obtener datos personales, de modo que no tiene mayor incidencia en el trabajador que los sistemas más tradicionales de tarjeta de control" —control de horario y jornada— (De La Puebla, 2017: 48).

Como muestra adicional y "cercana" de lo dicho, "un botón": la STSJ Cataluña 23.5.2015 (rec. 6212/2012), en un conflicto en la empresa SCHINDLER S.A. (dedicada a la fabricación y mantenimiento de aparatos elevadores), analiza el asunto relativo a la adopción de medidas de vigilancia y control por parte del empresario, en concreto, la instalación de un *acelerómetro* en los teléfonos móviles (*Blackberry*) de los trabajadores de la sección de mantenimiento que permite convertir fenómenos físicos (2 minutos sin movimiento) en señales acústicas; es decir, es un aparato que se encarga de captar el movimiento o la ausencia del mismo (en cuyo caso se envía una señal de emergencia a centro de control permanente), dispositivo que se complementa con un GPS que está integrado en el teléfono. Como indica la Sala Social catalana en la sentencia que se acaba de indicar (23.5.2015):

> Los trabajadores están obligados a llevar el acelerómetro; lo tienen que llevar siempre, incluso fuera de la jornada laboral, porque

> lo tienen que poner a cargar en sus casas; no se puede desconectar sino que se tiene que hacer con una aplicación de la que no tienen conocimiento los trabajadores; lo que sí se puede es desconectar el sonido (…). Se genera una situación de riesgo psicosocial (estrés) pues la circunstancia de que utilice la empresa un aparato de última tecnología para controlar el trabajo no puede tener la consecuencia de que fuera de la jornada laboral tengan incluso que en su domicilio familiar haya de continuar en una situación in vigilando del citado dispositivo para que esté en condiciones óptimas para su buen funcionamiento en la jornada laboral.

Así las cosas, comparto la opinión de que el derecho al descanso previsto tanto en el Derecho de la UE (Directiva 2003/88/CE) como en la normativa estatal (arts. 34 a 38 ET), supone que,si los empleados están «ilocalizables» y "no responden a su teléfono móvil o a los correos en sus ordenadores fuera del horario laboral, no se pueden calificar tales conductas como incumplimientos laborales sin que, por ende, quepa sancionarlas disciplinariamente" (Moreno González-Aller, 2018).

4. Hacia la consolidación de la desconexión digital como derecho laboral: avances reseñables y propuestas de cierre

La desconexión digital laboral o el derecho a la desconexión laboral es el "derecho de los trabajadores a desconectar del trabajo por medios digitales una vez finalizada la jornada laboral convenida" (López Garrido, Serrano Pérez y Fernández Aller, 2017: 60).

Como señala Moreno González-Aller (2018), "El Derecho de la Unión Europea impone que los conceptos de tiempo de trabajo, descanso, tiempo de presencia y trabajo efectivo, deban ser interpretados de manera uniforme en todo el ámbito comunitario, para garantizar eficazmente la aplicación de la normativa y la seguridad y salud de los trabajadores". No sólo eso, pues a este propósito debe recordarse que ya el art. 24 de la DeclaraciónUniv de DDHH de 1948 reconoce el "Derecho de «toda persona» al «descanso, al disfrute del tiempo libre, a una limitación razonable de la duración del trabajo»"; que el Pacto Internacional de Derechos Económicos, Sociales y Culturales (1966), en su art. 7.d), reconoce "disfrute de condiciones de trabajo que aseguren, en especial, "el descanso, el disfrute del tiempo libre, la limitación razonable de las horas de trabajo"; que el CV OIT núm. 30-1930 sobre horas de trabajo en comercio/oficinas, en su art. 2 (ratificado en el año 1932), indica que "Las horas de trabajo lo son mientras «el personal esté a disposición del empleador» , con exclusión de «los descansos durante los cuales el personal no se halle a la disposición del empleador» , indicando en su art. 3 que "«las horas de trabajo (...) no podrán exceder de cuarenta y ocho por semana y ocho por día»"; que el art. 31 de la Carta de Derechos Fundamentales de la UE indica que "todo trabajador tiene derecho a la limitación de la duración máxima del trabajo y a periodos de descanso diarios y semanales" (al respecto del descanso semanal, de interés es la lectura de la STJUE de 9.11.2017, asunto *Maio*), fijando la Directiva 2003/88 la "Duración semanal de la jornada en 48 horas, incluidas HE, en promedio anual, con período mínimo de descanso diario de 11 horas entre jornadas, descanso semanal ininterrumpido de 24 horas y permitiendo, la normativa española, jornadas especiales x sectores (RD 1561/1995, en el ámbito de la UE, de sumo interés es la STJUE 21.2.2018, asunto *Ville de Nivelles*, a propósito de las guardias domiciliarias de los bomberos) y por convenio colectivo CC (distribución irregular de la jornada —art 34.2 ET—).

De esta suerte, con toda claridad se ha escrito que, en España:

> La ausencia de regulación sobre un inexistente derecho a la desconexión digital en el entorno laboral no ha significado, ni mucho menos, una desprotección total y absoluta de los trabajadores frente a decisiones empresariales desproporcionadas. Esta laguna normativa ha sido en ocasiones colmada por nuestros tribunales, que han puesto coto a los excesos de conectividad por encima de la jornada ordinaria de trabajo (Talens Visconti, 2018).

Un avance importante en la senda del derecho a la desconexión digital (a mi juicio, un evidente *leading case)*, lo constituye la sentencia de la Audiencia Nacional de 17.7.1997 (proced

 ISSN: 2339-5753

120/1997), en la cual se declaró la nulidadde las instrucciones de la empresa que obligaban a los empleados a "mantener la atención a sus teléfonos móviles una vez finalizada la jornada de trabajo de cada uno de ellos".Un paso más, sin duda, lo constituyó la STS, Sala Social, de 21.9.2015 (rco. 205/2014), que declaró nula la cláusula de un contrato de trabajo que obligaba al trabajador a incluir teléfono móvil y e-mail personal para recibir comunicaciones "laborales" de la empresa, debiendo notificar los cambios posteriores, señalando el Alto Tribunal que no hay consentimiento libre y voluntario al firmar el contrato que incluye dicha cláusula, sino "*miedo*" a no ser contratado, apreciando el TS que se vulnera el derecho a la protección de datos de carácter personal (art. 18.4 CE).En esta senda, descuella, también, la STSJ Castilla y León de 3.2.2016 (AS 2016/99), que indica que las empresas que utilizan TIC o teletrebajo (en el domicilio o "a distancia") deberían disponer de políticas de gestión del tiempo (procedimientos de conexión, medios de control y registros de jornada), para afrontar reclamaciones sobre excesos de jornada, seguridad y salud laboral (exceso de conexión y estrés laboral, especialmente).

Un nuevo frente en cuanto a los límites temporales de la prestación se abre con la polémica en derredor del registro de la jornada diaria. La STS 23.3.2017 (u.d. 81/2016), ha señalado que el art. 35.5 ET "no exige la llevanza de un registro de la jornada diaria efectiva de toda la plantilla para poder comprobar el cumplimiento de los horarios pactados", sino sólo en los casos de trabajo a tiempo parcial o trabajo en sectores con jornadas especiales (ferroviarios, marina mercante, trabajadores móviles). Ello ha motivado el planteamiento de cuestión prejudicial por Auto de la Sala Social de la Audiencia Nacional el 19.1.2018 (asunto C-55/2018), que pregunta al TJUE, a propósito de la Directiva 2003/88, en clave de garantía de descanso semanal y diario, si resulta exigible no sólo a los trabajadores a tiempo parcial, ferroviarios, de marina mercante y trabajadores móviles, sino también a los empleados a tiempo completo, la existencia de un control diario de la jornada trabajada y de los excesos de jornada. Al cierre de este trabajo, está pendiente el pronunciamiento del TJUE, si bien la Comisión Europea, en sus alegaciones publicadas en fecha 19.7.2018, ha manifestado que el registro de la jornada diaria de todos los empleados es un mecanismo correcto en términos de dar cumplimiento al efecto útil de la Directiva 2003/88 (Comisión Europea, 2018); de su lado, no puede ignorarse que el 17.10.2017, se publicó en el Diario de Sesiones del Congreso de los Diputados (nº 82) la proposición de Ley del Grupo Parlamentario Socialistas, para incluir la obligación de registro diario de jornada y horario concreto de entrada y salida de cada trabajador (expediente 122/000109), que, orillado en su día (Miñarro, 2018), en el actual contexto legislativo podría ser retomado.

Por lo pronto, si existe tiempo de disponibilidad "tecnológica" (no desconectado), el mismo es tiempo de trabajo como una suerte de "guardia localizable", en especial cuando después de una llamada se deben prestar servicios (STJUE 3.10.2000, asunto *Simap*, STJUE 21.2.2018, asunto *Ville de Nivelles*), aunque sea "desde el domicilio" del trabajador y fuera de su jornada laboral (STJUE 5.10.2004, asunto *Pfeiffer*); mientras que si hablamos de "desconexión", dicho tiempo debe ser de descanso (sin obligación alguna para con el empleador —STJUE 9.9.2003, asunto *Jaeger*—) y no de disponibilidad tecnológica. De su lado, el tiempo de desplazamiento de los trabajadores móviles (tiempo diario de desplazamiento entre su domicilio y los centros del primer y del último cliente que les asigna su empresario) constituye «tiempo de trabajo», en el sentido de la Directiva 2003/88 (STJUE de 10 de septiembre de 2015, asunto *Tyco*).

El Derecho comparado nos enseña por dónde puede discurrir la futura regulación, en España, del derecho a la desconexión digital. Así, muy publicitado ha sido el caso de la Ley 2016/1088, de 8.8.2016 (vigente desde el 1.1.2017), relativa al trabajo, la modernización del diálogo social y las garantías de la carrera profesional, que introduce un nuevo apartado (art. L. 2242-8) en el *Code du Travail*en Francia, y es fruto de las reflexiones contenidas al respecto en el denominado *informe Mettling* (a la sazón, director gral. adjunto de la empresa de telefonía móvil ORANGE).

La regulación francesa puede explicarse con facilidad (Alemán Páez, 2017;Cialti, 2017;Di Meo, 2017;Ray, 2016): a) se prevé, en el marco de la negociación anual colectiva sobre la igualdad profesional de hombres y mujeres y calidad de vida, la inclusión de las modalidades de pleno

ejercicio por los trabajadores del "derecho a desconectar" y la regulación del uso de los dispositivos digitales (respeto del tiempo de descanso, vacaciones y vida personal/familiar); b) si no hay acuerdo colectivo, el empresario, previa audiencia del Comité de Empresa o de los delegados de personal, ha de elaborar una política de actuación al respecto, definiendo las modalidades de ejercicio del derecho a desconexión, poniendo en marcha acciones de formación/sensibilización sobre el uso "razonable" de los dispositivos digitales, dirigidas a los empleados, mandos intermedios y directivos. El problema de la normativa francesa, empero, es evidente: no están previstas "sanciones" en caso de incumplimiento empresarial.

En Italia, la Ley 81/2017, vigente desde el 14.6.2017, aborda el tratamiento de las nuevas formas de trabajo, denominadas ágiles, flexibles o *Smart work*, a modo de teletrabajo a tiempo parcial. Con carácter voluntario, puede acordarse entre trabajador y empresario y consiste en combinar tiempos de presencia en la empresa con tiempos de trabajo fuera de ella, con la posible utilización de instrumentos tecnológicos para el de desarrollo de la actividad laboral. En su artículo 19.1 se dispone que el acuerdo para dar paso a este "trabajo ágil" debe establecer los tiempos de descanso, así como las medidas técnicas y organizativas necesarias para asegurar la desconexión del trabajador de los instrumentos tecnológicos de trabajo (Charro, 2017; Di Meo, 2017; Talens, 2018).

Es verdad, además, que algunas empresas, como Volkswagen (bloqueo de acceso a comunicaciones corporativas vía móvil de 18.15 h. a 7 h.), Gie Réunica (bloqueo de recepción de e-mailsdesde las 20 horas a las 7 h., así como el fin de semana desde las 20 horas del viernes a las 7 horas del lunes siguiente), Daimler (software que eliminaba automáticamente todos los correos electrónicos recibidos durante las vacaciones de los trabajadores, con la respuesta automática *Mail on Holiday*y la indicacion del e-mail de otro empleado que no estuviera de vacaciones) o BMW (regulación colectiva del trabajo móvil conectado a una red —*vernetzte Mobilarbeit*—con derecho a "no estar disponible"salvo que se trate de "tiempo de disponibilidad" pactado dentro de la jornada ordinaria) han implantado políticas de desconexión. En España, el CC de AXA reconoce —art. 14, BOE 10.10.2017— el derecho a la desconexión digital, entendido del siguiente modo:

> El lugar de la prestación laboral y el tiempo de trabajo, como típicos elementos configuradores del marco en el que se desempeña la actividad laboral, están diluyéndose en favor de una realidad más compleja en la que impera la conectividad permanente afectando, sin duda, al ámbito personal y familiar de los trabajadores y trabajadoras. Es por ello que las partes firmantes de este Convenio coinciden en la necesidad de impulsar el derecho a la desconexión digital una vez finalizada la jornada laboral. Consecuentemente, 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.

Es claro que la negociación colectiva, de sector o de empresa, puede introducir medidas concretas que faciliten la desconexión digital (Charro, 2017), tanto como obligación de la empresa, como derechos y deber del propio empleado (para evitar un "vampirismo adictivo" a la tecnología en tiempo de descanso por motivos "profesionales"—*workaholics*—). En este sentido, se ha sugerido que la negociación colectiva de empresa (o acuerdos internos de empresa) puede acoger cláusulas relativas alcierre automático de los servidores de correo una vez finalizado el horario de trabajo y hasta el inicio del mismo al día siguiente, al establecimiento de periodos horarios en que se prohíbe el envío de correos electrónicos entre empleados, a recoger una nota recordatoria del derecho a la desconexión en los correos electrónicos, a concienciar a los empleados en la reducción del envío de correos electrónicos—vía formación obligatoria, por ejemplo en el marco de la prevención de riesgos laborales psicosociales—, entre otras (Pareja Frade, 2017).

En términos políticos, hace ya algún tiempo (BOCG-CD 7.4.2017, nº 139, serie D) que el PSOE propuso reformar la ley de Protección de Datos a través de una "enmienda de adición que incorpore, por primera vez, la garantía de los derechos digitales, entre ellos el derecho de los empleados a no tener que responder comunicaciones electrónicas fuera de su jornada legal de trabajo, garantizando así el respeto a su tiempo de descanso y vacaciones así como de su intimidad personal y

 ISSN: 2339-5753

familiar"(Moreno González-Aller, 2018). No debe desconocerse, tampoco, la Proposición no de Ley presentada por el Grupo Parlamentario Confederal de Unidos Podemos-En Comú-Podem-En Marea, sobre el *derecho a la desconexión laboral fuera del horario de trabajo* (BOCG-CD, 17.3.2017, núm. 125), que pretende evitar que "los trabajadores y trabajadoras puedan continuar trabajando después de finalizar su jornada laboral utilizando los medios electrónicos de la empresa", instando al Gobierno a desarrollar una regulación legal conjuntamente con los agentes sociales del *uso de las tecnologías de la comunicación* (mensajería y correos electrónicos o dispositivos móviles) *fuera de la jornada laboral* con el objetivo de evitar que los trabajadores y trabajadoras puedan continuar trabajando después de finalizar su jornada laboral, utilizando los medios electrónicos de la empresa, y garantizar la seguridad y salud en el trabajo y el descanso necesario, mediante la limitación de la jornada laboral y el respeto a las vacaciones de las personas trabajadoras, "educando" digitalmente a empresarios y empleados (entiendo que para afrontar el estrés y el *burnout* tecnológico).

Así las cosas y en conclusión: a) entiendo que *no es superfluo*, sino necesario, el reconocimiento del derecho a la desconexión digital, como singular especificación "tecnológica" del derecho al descanso laboral recogido en el art. 31 de la CDFUE, bien como derecho laboral básico (art. 4 ET), bien dentro de la regulación del tiempo de trabajo y descanso (arts. 34 a 38 ET), bien en ambos lugares normativos, fijando además que no sólo es un derecho de los trabajadores sino también un deber u obligación legal de las empresas (obligación cuya inobservancia podría tipificarse/sancionarse en el marco de la LISOS —RDLeg. 5/2000—), salvo casos excepcionales "de urgente necesidad o de guardias domiciliarias que sean consideradas como tiempo de trabajo" (Talens Visconti, 2018); b) en cuanto al contenido del derecho, comprendería tanto la no recepción de correos electrónicos tras la jornada laboral como la no conexión a Internet para cuestiones laborales, por medio de tablets, smartphones, información en la nube, etc. (López Garrido et al., 2017: 61); c) la legislación española podría "regular", además, la videovigilancia en la empresa (conectada a la jurisprudencia del TJUE y del TCo), sus límites y la protección de datos anudada, la implementación de GPS y sus límites,así como hacer una llamada (remisión en régimen de mejora, desarrollo y concreción práctica—técnica de suplementariedad y de complementariedad—) a la negociación colectiva, de sector (preferentemente) y/o de empresa, en orden a que incorporen cláusulas sobre uso de las TIC (profesional-personal, límites, información a los empleados, formación), sobre desconexión digital (en clave de derecho reconocido y, también, en clave de obligación, vía formación en prevención de riesgos laborales —afrontamiento de riesgos psicosociales por tecnoestrés—, para los empleados), pudiendo tal regulación ser completada,en cuestiones adaptativas puntuales,bien mediante acuerdo de empresa, bien mediante código corporativo de buenas prácticas.

Referencias

Alemán Páez, Francisco (2017): "El derecho a la desconexión digital".*Revista de Trabajo y Derecho*, 30, 12-33

Charro Baena, Pilar (2017): "Cambios tecnológicos y tiempo de trabajo". *Derechos Fundamentales y Tecnologías Innovadoras - Actas del III Encuentro Internacional sobre Transformaciones del Dereho del Trabajo Ibérico*, 20-27.

Cialti, C. Henri. (2017): "El derecho a la desconexión en Francia: ¿más de lo que parece". *Temas Laborales*, 137,163-181.

Comisión Consultiva Nacional de Convenios Colectivos (2017): "*El derecho a la desconexión y a la conciliación en la negociación colectiva*". Boletín, 57. Recuperado de: http://www.empleo.gob.es/es/sec_trabajo/ccncc/B_Actuaciones/Boletin/Nxmero_57_Marzo_2017.pdf

Comisión Europea (2018): *Alegaciones a la cuestión prejudicial C-55/2018.* Recuperado de: https://d1hd7hmh02y0fr.cloudfront.net/smartlex/pdf/Informe-Comision-Europea-registro-jornada.pdf

De La Puebla Pinilla, Ana (2017): "Geolocalización y control biométrico". *Derechos Fundamentales y Tecnologías Innovadoras - Actas del III Encuentro Internacional sobre Transformaciones del Dereho del Trabajo Ibérico*, 44-50.

Di Meo, Rosa (2017): "Il diritto alla disconnessione nella prospettiva italiana e comparata". *Labour & Law Issues*, 3-2, 18-38.

García Vitoria, Ignacio (2018): *La protección de datos como eje de la jurisprudencia del Tribunal de Estasburgo sobre la privacidad del trabajador y el control empresarial.*Recuperado de: http://eapc-rcdp.blog.gencat.cat/2018/02/28/la-proteccion-de-datos-como-eje-de-la-jurisprudencia-del-tribunal-de-estasburgo-sobre-la-privacidad-del-trabajador-y-el-control-empresarial-ignacio-garcia-vitoria/[consulta 26 de agosto de 2018]

López Cumbre, Lourdes (2018): *Vigilar ocultamente a los trabajadores en la empresa y la reciente doctrina del Tribunal Europeo de Derechos Humanos.*Recuperado de: http://www.gomezacebo-pombo.com/media/k2/attachments/vigilar-ocultamente-a-los-trabajadores-en-la-empresa-y-la-reciente-doctrina-del-tribunal-europeo-de-derechos-humanos.pdf [consulta 26 de agosto de 2018].

López Garrido, Diego.; Serrano Pérez, Maria Mercedes; Fernández Aller, Celia (2017): "Derechos y obligaciones de los ciudadanos/as en el entorno digital".*Fundación Alternativas,* 195. Recuperado de: http://www.fundacionalternativas.org/public/storage/laboratorio_documentos_archivos/d913d53f47205b4df8d1f60691ede39e.pdf[consulta 26 de agosto de 2018].

Mercader Uguina, Jesús Ramón (2001): "Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?" *Relaciones Laborales*, 1, 665-686.

Miñarro Yanini, Margarita (2018): "La «Carta de derechos digitales» para los trabajadores del Grupo Socialista en el Congreso: un análisis crítico ante su renovado interés". *RTSS- CEF*, 424,

Molina Navarrete, Cristóbal (2017):"El tiempo de los derechos en un mundo digital: ¿existe un nuevo derecho humano a la desconexión de los trabajadores fuera de la jornada?". *Revista de la Facultad de Derecho de México*, 269 (67), 891-919. https://doi.org/10.22201/fder.24488933e.2017.269.62482

Moreno González-Aller, I.gnacio (2018): "El derecho de los trabajadores a la desconexión tecnológica". *Revista de Jurisprudencia El Derecho.* Recuperado de https://elderecho.com/derecho-los-trabajadores-la-desconexion-tecnologica [consulta 26 de agosto de 2018].

Pareja Frade, Carlos (2017): *El derecho a la desconexión digital en España: un aspecto a negociar.* Recuperado de:http://www.legaltoday.com/practica-juridica/social-laboral/laboral/el-derecho-a-la-desconexion-digital-en-espana-un-aspecto-a-negociar [consulta 26 de agosto de 2018].

Preciado Domènech, Carlos Hugo (2017): "Nuevas formas de prueba basadas en las tecnologías de la información y la comunicación (TIC). Documento electrónico y prueba digital: Proposición y práctica. Ilicitud de estas pruebas por vulneración de derechos fundamentales". *Actum Social*, 131, 11-36.

Ray, Jean Emmanuel (2016): "Grande accélération et droit à la déconnexion". *Droit Social*, 11, 912-920.

San Martín Mazzuconi, Carolina (2017): "Generalización tecnológica: efectos sobre las condiciones de trabajo y empleo". *Derechos Fundamentales y Tecnologías Innovadoras - Actas del III Encuentro Internacional sobre Transformaciones del Dereho del Trabajo Ibérico*, 4-11.

Talens Visconti, Eduardo Enrique (2018): "La desconexión digital en el ámbito laboral: un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva". *Información Laboral*, 4, 1-17.

Todolí Signes, Adrià (2017): *El derecho a la desconexión digital ya existe. Nos venden humo si no se establecen sanciones claras para quien lo vulnere*. Recuperado de: https://adriantodoli.com/2017/03/29/el-derecho-a-la-desconexion-digital-ya-existe-nos-venden-humo-si-no-se-establecen-sanciones-claras-para-quien-lo-incumpla/[consulta 26 de agosto de 2018].

Todolí Signes, Adrià (2018): *La vigilancia electrónica de los trabajadores tras la nueva regulación de Protección de datos*. Recuperado de: https://adriantodoli.com/2018/06/12/la-vigilancia-electronica-de-los-trabajadores-tras-la-nueva-regulacion-de-proteccion-de-datos/[consulta 26 de agosto de 2018].

Vallecillo Gámez, Maria Rosa (2017): "El derecho a la desconexión: ¿«novedad digital» o esnobismo del «viejo» derecho al descanso?", *RTSS-CEF*, 408.

Ushakova, Tatiana (2016): "De la conciliación a la desconexión tecnológica. Apuntes para el debate". *Nueva Revista Española de Derecho del Trabajo*, 192, 117-138.