TIC i protecció de dades en la relació laboral

PID_00248473

Miguel Ángel Purcalla

Temps mínim de dedicació recomanat: 3 hores

Universitat Oberta de Catalunya

Miguel Ángel Purcalla

Magistrat jutge del Social. Professor titular de universitat (en excedència voluntària). Doctor en Dret.

Índex

Introducció

La incidència de la tecnologia (ja no nova, tot i que sí actual i en evolució constant) en la relació laboral es pot enfocar des de diversos punts de vista: l'empresari pot fer servir la tecnologia com a eina de producció, però també com a medi de control (videovigilància, programes espia informàtics, geolocalització, etc.); l'empleat utilitza la tecnologia que, quan la hi facilita l'empresa, pot / ha de seguir certes pautes (ús correcte i no il·lícit ni contraindicat, per exemple), i no perd certs drets (intimitat/privacitat, per exemple, o protecció de dades) pel fet de pertànyer a l'empresa. A aquestes qüestions es dedica, des del punt de vista normatiu i judicial, el present mòdul, des d'una perspectiva d'anàlisi.

Objectius

Els objectius que l'estudiant ha d'assolir després de treballar aquests materials didàctics són els següents:

1. Analitzar els límits del control empresarial de l'ús de les TIC per part dels empleats.

2. Valorar si és possible controlar tecnològicament el temps de treball dels empleats «mòbils» (geolocalització).

3. Analitzar casos reals sobre el conflicte entre l'interès empresarial i la privacitat/intimitat dels empleats en el cas de l'ús de TIC.

4. Distingir les claus d'ús «sindical» de les TIC a l'empresa.

1. Relació laboral, TIC i drets fonamentals (intimitat inclosa)

1.1. Relació laboral i drets fonamentals

La incidència de la **relació laboral en l'exercici dels drets fonamentals** ha estat reiteradament analitzada per la doctrina jurisprudencial, de la qual l'STS 2015.09.21 (u. d. 259/2014) és un exponent preclar, segons la qual els criteris bàsics són els següents:

1) La celebració d'un contracte de treball no implica la privació –per al treballador– dels drets que la Constitució li reconeix com a ciutadà, així com tampoc la llibertat d'empresa (art. 38 CE) justifica que els empleats «hayan de soportar limitaciones injustificadas de sus derechos fundamentales, porque el ejercicio de las facultades organizativas del empresario no puede traducirse en la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador». Així doncs, els drets fonamentals del treballador són prevalents i constitueixen un «límit infranquejable» no només a facultats sancionadores de l'empresari, sinó també a les seves facultats d'organització i de gestió, tant causals com discrecionals[1].

(1)SSTC 94/1984, de 16 d'octubre, 171/1989, de 19 d'octubre, 186/1996, de 25 de novembre, 196/2004, de 15 de novembre, 125/2007, de 21 de maig, i 56/2008, de 14 d'abril.

2) «Dada la posición preeminente de los derechos y libertades constitucionales en el ordenamiento jurídico, la modulación que el contrato de trabajo pueda producir en su ejercicio habrá de ser la estrictamente imprescindible para el logro de los legítimos intereses empresariales y proporcional y adecuada a la consecución de tal fin»[2]. Així doncs, en definitiva, «los equilibrios y limitaciones recíprocos que se derivan para ambas partes del contrato de trabajo suponen [...] que también las facultades organizativas empresariales se encuentren limitadas por los derechos fundamentales del trabajador, quedando obligado el empleador a respetarlos»[3], i «desde la prevalencia de tales derechos, su limitación por parte de las facultades empresariales solo puede derivar, bien del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho[4], bien de una acreditada necesidad o interés empresarial, sin que sea suficiente su mera invocación para sacrificar el derecho fundamental del trabajador»[5].

(2)SSTC 6/1982, de 21 de gener, 106/1996, de 12 de juny, 204/1997, de 25 de novembre, 1/1998, de 12 de gener, 90/1999, de 26 de maig, 98/2000, de 10 d'abril, 80/2001, de 26 de març, 20/2002, de 28 de gener, 213/2002, de 11 de novembre, i 126/2003, de 30 de juny.

(3)STC 292/1993, de 18 d'octubre.

(4)SSTC 99/1994, d'11 d'abril, i 106/1996, de 12 de juny.

(5)SSTC 99/1994, d'11 d'abril, 6/1995, de 10 de gener, 136/1996, de 23 de juliol, i 181/2006, de 19 de juny.

3) En síntesi, s'ha d'afirmar que si bé «por una parte, los derechos fundamentales del trabajador "deben adaptarse a los requerimientos de la organización productiva en que se integra"; [...] por otra parte, [...] también "las facultades empresariales se encuentran limitadas por los derechos fundamentales del trabajador"». D'aquesta manera, el contracte de treball no és títol legitimador de retallades en l'exercici dels dret fonamentals que afecten el treballador com a

(6)Art. 1.1 CE, STC 88/1985, de 19 de juliol.

(7)SSTC 151/2004, de 20 de setembre, i 56/2008, de 14 d'abril.

ciutadà, perquè la centralitat dels drets fonamentals en el sistema jurídic constitucional determina que limitin el poder de direcció de l'empresari, i perquè les organitzacions empresarials «no formen mons separats i estancs» d'una societat que viu conformada per un mateix text constitucional, i perquè les «manifestaciones de "feudalismo industrial" repugnan al Estado social y democrático de Derecho y a los valores superiores de libertad, justicia e igualdad a través de los cuales ese Estado toma forma y se realiza»[6]. Però també la «efectividad de los derechos fundamentales del trabajador en el ámbito de las relaciones laborales debe ser compatible [...] con el cuadro de límites recíprocos que pueden surgir entre aquellos y las facultades empresariales, las cuales son también expresión de derechos constitucionales reconocidos en los artículos 33 y 38 CE»[7].

Una qüestió ben diferent és que els drets, per fonamentals que siguin, no sempre són absoluts, sinó que poden ser modulats en el marc/context de la relació laboral. Fixeu-vos, per exemple, que la llibertat d'expressió no és il·limitada i menys «a l'empresa», en tant que determinades expressions que resulten perfectament legítimes en un altre context, deixen de ser-ho quan existeix un contracte de treball, ja que aquest genera una sèrie de drets i obligacions recíproques entre les parts que han de guiar-se per la bona fe, a més que la difusió lliure de pensaments, idees i opinions (a Facebook, Twitter, televisió, premsa o via WhatsApp), incloguin o no actes de «crítica», acaba on comença el dret a la dignitat i l'honor d'altres persones[8]. Així doncs, no és admissible, per exemple, l'insult gratuït als altres[9] ni expressions ofensives o ultratjants (injúries o calúmnies molt menys[10], sense perjudici que això hagi de ser ponderat en cada cas concret[11].

Com a mostra del que s'ha dit («no tot s'hi val» en l'ús de les xarxes socials, com Facebook o Twitter, o de WhatsApp), valgui un «botó introductori».

[8]STS 2013.02.12 –rec 254/2011–, STEDH 2017.02.21, assumpte *Paulina Rubio versus España*.

[9]STSJ Galícia 17.10.2008 –Regl. 360/2008.

[10]STSJ Galícia 2014.10.08 –Regl. 2941/2014.

[11]STS, Sala Social, 2016.12.22 –u. d. 201/2015–, assumpte *Apprece*.

L'STSJ Catalunya 2014.11.07 (Regl. 2817/2014)

Analitza el cas de l'acomiadament disciplinari (declarat procedent) d'una professora d'un centre infantil (llar d'infants) que va pujar la foto d'un nadó i, a partir d'aquesta les integrants del grup de WhatsApp van començar a fer comentaris jocosos i de contingut sexual sobre els atributs del menor. Arran d'això, el centre va acomiadar disciplinàriament la treballadora que va fer la fotografia i la va enviar, així com la directora, que es va sumar als comentaris i va permetre aquest comportament. Per contra, la resta de participants van rebre una sanció menor.

El tribunal va considerar que no tenia cap efecte atenuant el fet que els comentaris tinguessin lloc fora de l'horari laboral, ja que el que ha sancionat l'empresa no és una pèrdua de temps durant la jornada, sinó l'acció de fer una foto a un nadó, enviar-la per WhatsApp i proferir expressions amb una elevada càrrega sexual, conducta molt greu i culpable que, a més, atemptaria contra la protecció de dades i imatge del menor.

La directora va ser acusada de certa culpabilitat *in vigilando* i se li va imputar un plus d'exemplaritat sobre la resta de participants, per la qual cosa la sentència va adduir que la seva obligació hauria d'haver estat tallar d'arrel la conversa en lloc

de sumar-s'hi (de fet, la persona que va impugnar l'acomiadament a la sentència ressenyada va ser precisament la directora).

Tenint en compte el que s'ha dit, s'han de portar a col·lació les lúcides (i contundents) reflexions del magistrat R. López Parada, com a ponent de la sentència de l'Audiència Nacional de data 2014.05.27 (proced. 83/2014):

«[...] la rápida evolución de la tecnología en el ámbito de la comunicación y las redes sociales que permiten la socialización de las personas, también en el entorno de trabajo, exigen de la adaptación *pari passu* de las respuestas jurídicas, para lo cual han de aplicarse a fenómenos nuevos los valores que informan las instituciones laborales y los derechos fundamentales, como hizo el Tribunal Constitucional en su reiteradamente citada sentencia 281/2005. Ha de rechazarse por ello cualquier planteamiento "originalista", que congele los derechos fundamentales en el estado de la tecnología existente en el momento en que se dictaron las normas constitucionales, puesto que no en vano el artículo 3.1 del Código civil nos dice que las normas han de interpretarse en consideración a "la realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquellas", exigencia de actualización interpretativa que ha de ser más rigurosa cuando se trata de la protección de los derechos fundamentales reconocidos constitucionalmente. A ello ha de añadirse que la difusión social del uso de la tecnología va convirtiendo en notorio el conocimiento de los fundamentos tecnológicos y estructurales de tales sistemas de comunicación, que han dejado de ser patrimonio de unas élites tecnológicas para ser incorporadas a la vida cotidiana de millones de ciudadanos. Los órganos judiciales no pueden permanecer ajenos a dicha evolución social y dejar de apreciar como notorios los elementos básicos que configuran el funcionamiento de estos sistemas, como necesario punto de partida para dictar sus resoluciones».

1.2. TIC i relació laboral

És més que evident que els sistemes telemàtics projecten la seva influència en múltiples esferes del món del treball. Així doncs, n'hi ha prou a assenyalar:

- La implementació de sistema de teletreball com a mètode d'organització de la prestació (en línia, a distància o semipresencial).

- L'automatització de milers de processos de producció (robòtica, enginyeria electrònica, etc.), la remissió electrònica de nòmines i els seus justificants de pagament[12], que els treballadors poden imprimir introduint al terminal informàtic el seu DNI i una clau).

(12)STS 2016.01.12 (u. d. 3690/2014).

- L'emplenament de tràmits amb les TGSS (sistema xarxa) o en relació amb els accidents de treball (sistema CoNTA[13], a Catalunya, o sistema Delta).

(13)STC 211/2012, de 14 de novembre.

Per no parlar d'un cas més singular, que no és teletreball precisament, sinó ***crodwork offline***, una nova forma de **descentralització productiva**: les empreses «tecnològiques» (normalment anomenades *start-up*) posen en contacte el client que sol·licita una prestació de serveis amb el proveïdor per mitjà d'una **plataforma web** que conté una mena de **macrobase de dades**. Així doncs, el client contacta directament amb la persona (col·laborador «autònom» per a aquestes «empreses») que realitzarà la prestació al nucli local més proper al sol·licitant del servei.

Exemples d'això? Es pot pensar en:

- Uber, transport de passatgers, que segons la Comissió Europea és una «barreja entre plataforma digital i empresa de serveis», però segons el TJUE és una empresa de serveis de transport[14], cosa que afectarà d'altres empreses, com Cabify.

- Myfixpert, reparació d'aparells electrònics.

- Chefly, cuina a domicili.

- Helpling, neteja de la llar, que va iniciar la seva activitat a Espanya al novembre del 2014 i va tancar tot just un any més tard.

- D'altres com Deliveroo, Just Eat, Airbnb, Wimdu, TripAdvisor, Booking, HolidayCheck, etc.: el dubte sobre elles és si la seva regulació jurídica (laboral) serà diferent a partir del cas Uber i els criteris del TJUE.

(14)El TJUE ha dictat sentència, amb data de 20 de desembre del 2017, assumpte *Associacio Professional Èlit Taxi i Uber Systems Spain S. L.*, a propòsit de la qüestió prejudicial plantejada pel Jutjat Mercantil núm. 3 de Barcelona, indicant que Uber «no se limita a conectar usuarios con conductores a través de un sistema de intermediación de servicios de teléfonos inteligentes, sino que "crea al mismo tiempo una oferta de servicios de transporte urbano, que hace accesible concretamente mediante herramientas informáticas, como la aplicación controvertida en el litigio principal, y cuyo funcionamiento general organiza en favor de las personas que desean recurrir a esta oferta para realizar un desplazamiento urbano"».

Ara bé, aquesta realitat ve acompanyada d'una altra no menys important: la contraposició entre l'interès empresarial en l'**ús correcte i controlat** de les TIC en el marc de la relació laboral i els drets fonamentals de l'empleat que utilitza.

Respecte a aquesta qüestió, l'article 20.3 ET permet a l'empresari adoptar les mesures que consideri **més oportunes** de vigilància i control **per verificar el compliment per part del treballador de les seves obligacions i deures laborals**, tot i que ha de guardar en la seva adopció i aplicació la consideració corresponent a la dignitat i a la intimitat del treballador. Com a contrapunt, l'article 4.2.e ET reconeix el dret del treballador al **respecte de la seva intimitat i a la consideració de la seva dignitat** en la relació de treball.

A partir d'aquesta dada normativa, la **irrupció de les tecnologies** (ja no «noves», per descomptat, i encara que se les segueixi anomenant així, no només en l'àmbit laboral sinó en tots els àmbits de la societat ja no formen part d'un «imaginari» popular o d'un món distòpic, sinó de la vida quotidiana –mòbils, tauletes, ordinadors, etc.– de milions de persones) és una realitat consolidada la principal polèmica de la qual, en el marc laboral, fa referència a un doble tipus de qüestions:

a) En primer lloc, en relació amb el control de les comunicacions dels treballadors, en general i de l'ús d'equips informàtics, en particular.

b) En segon lloc, a la videovigilància/audiovigilància dels llocs de treball. Sobre aquestes i altres qüestions es parlarà als apartats següents.

2. Protecció i seguretat de dades personals en les relacions laborals

2.1. Normativa aplicable i reflexions introductòries

En el dret de la UE (art. 8 CDFUE i Reglament 679/2016), el **dret a la protecció de dades personals** es defineix com el «dret de tota persona física identificada o identificable al fet que la informació sobre si mateixa (incloses dades de localització, identificacions en línia o elements de la identitat genètica) sigui objecte de tractament per a fins concrets i només a partir del seu consentiment o un altre fonament legítim legalment establert».

En el dret intern, l'article 18.4 CE disposa que la llei **limitarà l'ús de la informàtica** per garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets.

A partir de l'STC 292/2000, de 30 de novembre, el TC distingeix nítidament el **dret a la protecció de dades personals del dret a la intimitat**, que s'erigeix com a dret fonamental autònom: «El objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo». El coneixement o l'ocupació d'aquestes dades per part de tercers pot afectar els seus drets, siguin o no fonamentals, perquè el seu objecte no és només la intimitat individual, que ja està protegida a l'article 18.1 CE, sinó les dades de caràcter personal.

Article 18.4 CE

Aquest article es desenvolupa a l'LO 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD), que va ser desenvolupada des del punt de vista reglamentari per l'RD 1720/2007, de 21 de desembre, i per l'RD 429/1993, de 26 de març, que va aprovar l'Estatut de l'Agència Espanyola de Protecció de Dades.

La normativa laboral no conté una previsió específica que estableixi els drets i deures dels treballadors en l'àmbit de la protecció de dades. De totes maneres, convé fer una sèrie de consideracions en aquest sentit:

1) El treballador que entra en contacte amb **dades personals de tercers**, en el marc de la seva prestació de serveis, realitza una activitat de **«tractament de dades»**, definida a l'article 3.c de l'LOPD així: «Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias».

2) El treballador que realitza el tractament de dades per compte del seu ocupador s'equipara a la figura de l'«**encarregat del tractament**», definit a l'article 3.g de l'LOPD amb aquestes paraules: «[…] la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento».

3) El tractament de dades personals que realitza un treballador per compte del seu ocupador no constitueix un acte de «**cessió de dades**», però la intervenció del treballador és equiparable a la de l'«encarregat del tractament». És a dir: per la seva intervenció en el tractament de dades, el treballador assumeix les responsabilitats de custòdia i seguretat inherents a la figura de, com diu l'article 9.1 LOPD, l'«encargado del tratamiento, que incluyen el deber de protección de datos personales». Per tant, els treballadors que participin en el tractament de dades personals tenen el deure d'actuar seguint les instruccions de l'ocupador, que és el responsable de les dades i, com a tal, té el deure d'organitzar-se per complir amb les previsions de la LOPD (seguretat de les dades, confidencialitat).

4) L'incompliment voluntari del «**deure de protecció de dades personals**» suposa una transgressió de la bona fe i encaixa en la conducta que preveu l'article 54.2 ET (acomiadament disciplinari). Serien conductes sancionables:

a) Arxivar i/o publicar salaris de tota o part de la plantilla, de registres de jornada, de la relació de personal, de telèfons de contacte, quadre de vacances de tota la plantilla, etc.[15]

(15)STSJ Catalunya 6.4.2009 (Regl. 380/2009) i STSJ Madrid 2015.11.30 (rec. 454/2015).

b) Enviar reiteradament certificats mèdics a comptes de correu electrònic alienes a l'empresa[16].

(16)STSJ Galícia 2012.11.23 (Regl. 4009/2012).

c) Utilitzar les dades d'un altre treballador per atribuir-li la comissió d'infraccions de trànsit[17].

(17)STSJ Madrid 2015.02.25 (Regl. 785/2014).

Ara bé, en aquells casos en què els companys de feina autoritzen la manipulació o revelació de les seves dades o es pot deduir que existeix aquesta autorització, la doctrina judicial ha considerat que la infracció de l'LOPD no justifica l'acomiadament (STSJ Aragó 1.10.2008 Regl. 691/2008).

També serien motiu d'acomiadament disciplinari, com a regla general, la cessió de dades de tercers (clients, proveïdors, socis) per part de treballadors[18], tot i que no sempre és així, ja que es requereix que aquesta cessió o apropiació indeguda de dades tingui prou entitat per ser considerada com a causa d'acomiadament[19].

(18)Per exemple, STSJ País Basc 2013.06.04 (Regl. 940/2013), STSJ Andalusia-Màlaga 2015.04.23 (Regl. 423/2015), SSTSJ Catalunya 2013.12.09 (Regl. 4344/2013) i 2015.09.24 (Regl. 3275/2015), i STSJ Madrid 2016.01.27 (Regl. 921/2015).

(19)Per exemple, no és improcedència per a l'STSJ Castella-la Manxa 2011.04.14 (Regl. 324/2011) i STSJ Andalusia-Granada 2012.10.04 (Regl. 1660/2012).

Així, per exemple, s'ha arribat a declarar la improcedència del comiat en el cas analitzat per la STSJ de Catalunya, Sala Social, de 3 de desembre del 2015 (Rº 3254/2015), en la qual una empleada d'un hospital va utilitzar dades de pacients per a incloure'ls en la seva tesi doctoral i els va treure de l'hospital en què prestava els seus serveis sense tenir l'autorització de la seva empleadora ni dels pacients referenciats.

La STJUE de 30 de maig del 2013 (assumpte *Worten*) analitza l'adopció, per part d'una empresa privada, d'un sistema d'accés restringit als registres de temps de treball del personal laboral, de forma que l'empleador podia tenir accés automàtic a aquesta informació. El TJUE indica que l'esmentat registre, «en tanto en cuanto indica las horas en que cada trabajador inicia y finaliza la jornada, así como las pausas o períodos de descanso correspondientes, e identifica o hace identificable al individuo, queda comprendido en el concepto de datos personales», de forma que aquesta recollida, emmagatzematge i ús de les dades per l'empleador, així com la seva transmissió a autoritats nacionals competents en matèria de supervisió de les condicions de treball constitueixen un tractament de dades personals. El TJUE també repassa els principis de protecció de dades que han de ser aplicats en el tractament d'aquesta informació (recollits amb fins determinats, explícits i legítims, adequats, pertinents i no excessius). Igualment, la STJUE d'11 de desembre del 2014 (assumpte *Frantisek Rynes*) indica que «la grabación en vídeo de imágenes de personas que se almacenan en un dispositivo de grabación continuada, a saber, el disco duro de la empresa, constituye un tratamiento automatizado de datos personales».

2.2. El «poder de vida laboral» de les dades mèdiques

Un cas molt habitual ens permet situar-nos al principi d'aquesta qüestió. Pel que fa a l'accés a la selecció per a un lloc de treball, la doctrina judicial, a propòsit del «poder de vida laboral» dels informes mèdics, ha assenyalat que si la superació d'un reconeixement mèdic (apte/no apte) és requisit obligatori, d'acord amb les bases de la convocatòria[20], per accedir, per mitjà d'un procés selectiu, a una plaça fixa en una empresa pública, el jutjat **no pot qüestionar un element tècnic** com és una valoració mèdica d'aptitud, llevat que hi hagi un errors evident[21].

(20)No impugnades (fet que podria fer-se, per exemple, via conflicte col·lectiu, com assenyalen l'STSJ Astúries 30.9.2011 –Regl. 2189/2011– i l'STS 2012.11.07 –RJ 2012/8975–), cosa que equival a la seva acceptació tàcita per a qui participa en el procés selectiu (SSTS 1985.12.07 –RJ 1985/5936–, 1987.06.27 –RJ 1987/4304– i 1991.06.14 –RJ 1991/6240).

(21)STSJ Andalusia-Sevilla 23.1.2007 (Regl. 3801/2005).

Què passa a la pràctica?

Que no és el mateix que el metge conegui el motiu de la no aptitud que l'empresa el pugui conèixer, ja que aquesta, d'acord amb l'article 22 LPRL (cal recordar que l'accés a l'historial mèdic complet se circumscriu al treballador i al personal sanitari, d'acord amb el principi de confidencialitat), només pot

(22)Informe 209/2009 de l'AEPD.

saber si és apte o no (és a dir, tenir accés a les «conclusions» de l'informe mèdic –aptitud o no–, i serà el servei de prevenció el responsable del tractament de les dades[22]).

Una qüestió diferent és que sol ser habitual que l'informe mèdic digui que **no és idoni per a una tasca X, però això no vol dir que no sigui apte per a altres**. Aquesta distinció[23] està relacionada, per exemple, amb una incapacitat permanent parcial (algunes tasques de la professió habitual no es poden fer però sí altres), amb un reconeixement mèdic previ obligatori a activitats amb risc de malaltia professional (art. 196 LGSS 1994 i 243 LGSS 2015), amb una adaptació del lloc de treball, amb una recol·locació[24] o amb un acomiadament per ineptitud sobrevinguda (art. 52.a ET) coneguda amb posterioritat a l'ingrés a l'empresa i que impedeixi totalment el desenvolupament de l'activitat habitual.

(23)«No apte» no és el mateix que «no idoni per a» alguna tasca concreta d'un lloc de treball o grup professional.

(24)Especial sensibilitat sobrevinguda ex article 25 LPRL.

Sense oblidar, tampoc, que l'empresari està obligat a compatibilitzar els seus deures preventius amb la regla general de sol·licitar el consentiment informat del treballador sobre les proves concretes que se li hagin de realitzar en el context de la vigilància de la seva salut[25].

(25)Art. 22 LPRL, STC 196/2004, de 15 de novembre.

El tema mèdic, però, és diferent al relatiu a la facilitació de la representació legal dels treballadors (RLT) de documents relatius a un accident de treball/malaltia professional (AT/EP). En aquest cas, l'STS 2016.02.24 (rec. 79/2015) assenyala el dret d'un delegat de prevenció a accedir als informes i documents resultants de la investigació dels AT/MP realitzats per l'empresa (art. 36.2.b LPRL), «puesto que estos informes forman parte del proceso global de evaluación de riesgos laborales, sin perjuicio de las limitaciones derivadas, entre otras materias, de la protección de datos de carácter personal de los trabajadores afectados».

Finalment, resulta d'especial interès el coneixement empresarial, si més no en la seva mínima expressió, d'un estat de malaltia «crònica» o perllongada d'una persona, ja que sabut és que el Tribunal Suprem fa temps que sosté que la malaltia, des d'una perspectiva estrictament funcional d'incapacitat per al treball, que fa que el contracte de treball no es consideri rendible per a l'empresa, **no és un factor discriminatori** en el sentit estricte que aquest terme té en l'incís final de l'article 14 CE, encara que pogués ser-ho en altres circumstàncies en què **resulti apreciable l'element de segregació**[26]. Per la seva banda, les SSTC 62/2008, de 26 de maig, i 36/2011, de 28 de març, han assenyalat que perquè l'estat de salut d'un treballador, o més pròpiament la seva «malaltia», pugui constituir un factor de discriminació, cal que **la patologia constitueixi l'element determinant del comportament empresarial**.

(26)SSTS de 12 de juliol del 2004 (4646/2002), 23 de maig del 2005 (2639/2004), 22 de novembre del 2007 (3907/2006), 11 i 18 de desembre del 2007 (4355 i 4194/2006), 22 de gener del 2008 (3995/2006), 13 de febrer del 2008 (4739/2006) i 27 de gener del 2009 (602/2008), 22 de novembre del 2007 (3907/2006), 22 de setembre del 2008 (3591/2006) i 27 de gener del 2009 (602/2008).

El TJUE ha assenyalat que la **malaltia** no pot considerar-se, com a regla general, una de les causes de discriminació prohibides, ni és assimilable sense més a la discapacitat com a causa de discriminació[27], llevat que tal malaltia sigui

(27)STJCE 11.7.2006, assumpte *Chacón Navas*.

greu, entesa com a crònica o de llarga durada[28]; per exemple, l'obesitat en si no és una malaltia equiparable a discapacitat (com afirma la Directiva 2000/78, sobre igualtat de tracte en l'ocupació), però podria estar inclosa en la noció de discapacitat en el supòsit següent: «Cuando acarreara una limitación, derivada en particular de dolencias físicas, mentales o psíquicas que, al interactuar con diversas barreras, pudiera impedir la participación plena y efectiva de dicha persona en la vida profesional en igualdad de condiciones con los demás trabajadores, y si esta limitación fuera de larga duración»[29].

(28)Assimilable, en aquest sentit, a discapacitat (STJUE 2013.11.04, assumptes C-335/11 i 337/11, *HK Danmark*, I STJUE 2016.01.12, assumpte *Daouidi*).

(29)STJUE 2013.12.18, assumpte C-354/13.

Així doncs, cal prendre nota del criteri del TJUE amb vista a calibrar el que serà cada vegada més habitual: la presa en consideració de la malaltia crònica que comporti limitacions físiques o psíquiques com a situació assimilable a la discapacitat.

2.3. Sobre les dades tecnologicopersonals que cal incloure al contracte de treball

En aquest apartat s'ha de fer una menció obligada a l'STS 2015.09.21 (u. d. 259/2014).

S'hi recull el cas d'un «model tipus» de contracte laboral utilitzat per una empresa que conté una clàusula que preveu la cessió de dades personals del treballador a l'empresa (en concret, el telèfon personal i el correu electrònic) perquè l'empresa pogués comunicar-se amb el treballador, per SMS o correu electrònic, per «qualsevol assumpte relacionat amb el contracte de treball o la relació laboral».

Aquesta clàusula es declara nul·la per abusiva[30] ja que **anteposa la llibertat d'empresa** al dret a la protecció de les dades personals del treballador. En aquest sentit, interessa destacar que, d'acord amb l'article 6.2 LOPD i l'article 2.2 RD 1720/2007, el consentiment no s'exigeix en el marc del contracte de treball, ja que algunes dades personals (DNI o NIE, domicili, data de naixement o, per abonament de la nòmina, el compte corrent bancari, sens perjudici, per exemple, que la còpia bàsica només pugui contenir nom i cognoms del treballador, la seva data d'alta a l'empresa i el lloc o categoria que ha d'exercir[31], a més de les dades relatives a la retribució[32]) són necessaris per al perfeccionament del contracte de treball, que és una mena de «contracte d'adhesió» en què el treballador no té precisament gaire alternatives si vol accedir a l'ocupació. Però altres dades, com les referents a la clàusula tipus indicada, no són dades professionals, sinó personals, atès que no són ni el telèfon ni el correu electrònic facilitats per l'empresa, sinó que són els del mateix treballador. Ara bé, el dubte raonable que sorgeix és si aquesta doctrina (prohibició d'aquesta clàusula tipus en el contracte de treball) seria admissible en un

(30)Per la SANac 2014.01.28 (AS 2014/231).

(31)STC 142/1993.

(32)STJUE 2006.10.03, assumpte *Cadman*.

moment posterior a la signatura del contracte, un cop vigent la relació laboral, ja que el **consentiment ulterior** de l'actor bé podria interpretar-se com a vàlid per a facilitar aquestes dades.

Una qüestió vinculada a l'anterior és la relativa a si, un cop obtingudes, és apropiat **cedir dades tecnològicopersonals del treballador**. Doncs bé, entès que seria aplicable la lletra *c* de l'article 11.2 LOPD:

> «[...] cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación solo será legítima en cuanto se limite a la finalidad que la justifique».

Així doncs, seria possible la comunicació o notificació de dades personals del treballador a **organismes administratius**, per exemple, a l'oficina d'ocupació o de la Seguretat Social, però també, en un pla *inter privatos*, **des de l'ETT a l'empresa client o usuària**.

Molt al contrari, és obvi que resulta **il·lícit**, per vulneració del dret a la protecció de dades personals i del dret a l'honor, que una empresa comuniqui a una altra la causa de l'acomiadament d'un treballador, per tal de **incloure'l en una «llista negra»**, ja que això, a més, dificultarà la recerca de feina al treballador, i més si s'esdevé la situació següent: «tal cesión no contó con el consentimiento del afectado y dado que los datos no eran veraces y afectaban negativamente a su reputación»[33].

(33)STS, Sala Civil, 2015.11.12 (rec. 899/2014), que fixa una indemnització de 30.000 €.

2.4. Videovigilància i protecció de dades

L'**STCO 29/2013, d'11 de febrer**, analitza la videovigilància en relació amb el dret a la protecció de dades de caràcter personal (art. 18.4 CE, LO 15/1999 i RD 1720/2007).

En el cas analitzat, es va declarar afectat aquest dret i, per tant, es va considerar nul·la la prova de captació d'imatges del treballador en «lugares públicos de paso a fin de controlar su actividad laboral (control de puntualidad), porque ni el trabajador mismo, ni el comité de empresa habían sido informados del establecimiento de un sistema de control de la actividad laboral».

En aquesta sentència, es parteix del fet que **les imatges gravades en un suport físic constitueixen dades de caràcter personal** que queden integrades en la cobertura de l'article 18.4 CE, ja que el dret fonamental amplia la garantia constitucional a totes les dades que identifiquin o permetin la identificació de la persona i que puguin servir per a la confecció del seu perfil (ideològic, racial, sexual, econòmic o de qualsevol altra índole) o per qualsevol altra utilitat que, en determinades circumstàncies, constitueixi una amenaça per a l'individu[34], la qual cosa, com és evident, inclou també aquells que faciliten la

(34)STCO 292/2000, de 30 de novembre (F. 6).

identitat d'una persona física per mitjans que, amb imatges, permetin la seva representació física i identificació visual o ofereixin una informació gràfica o fotogràfica sobre la seva identitat.

La il·legalitat de la conducta empresarial no desapareix pel fet que l'existència de les càmeres fos apreciable a simple vista, ja que, d'acord amb l'esmentada STCO 29/2013,

> «no contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida».

Així doncs, el dret fonamental a la protecció de dades (art. 18.4 CE) va ser vulnerat amb la utilització no consentida ni prèviament informada dels enregistraments per a un fi, desconegut pels treballadors, de control de la seva activitat laboral.

En efecte, el TC va considerar que el tractament de les dades per a la supervisió laboral associada a les captures de la seva imatge **exigia una informació prèvia, expressa, precisa, clara i inequívoca** als treballadors sobre la captació d'imatges, la seva finalitat de control de l'activitat laboral i la seva possible utilització per a la imposició de sancions disciplinàries per incompliments del contracte de treball.

La Sentència Tco 39/2016, de 3 de març (assumpte *Inditex*), entén que un dispositiu de gravació de caixa registradora, sense prèvia comunicació als treballadors, és vàlid per a acomiadar a qui comet una falta laboral en l'ús d'aquesta caixa si a la botiga existien distintius informatius en un lloc visible sobre l'existència de càmeres instal·lades. Canvia, així, el criteri de la STCo 29/2013. Finalment, la STEDH de 28 de novembre del 2017 (assumpte *Antovic i Mirkovic contra la Universitat de Montenegro, Facultat de Matemàtiques*) entén que la gravació permanent amb videocàmeres de les classes dels professors d'aquesta escola vulnera la seva vida privada i intimitat, i no està justificada ni és proporcionada.

3. Control de les eines TIC corporatives per part de l'empresari

Aquest control consisteix en l'**accés al correu electrònic, a l'ordinador i a la navegació per internet del treballador per part de l'empresari**.

La generalització de l'ús d'ordinador (correu electrònic, internet i xarxes socials) en el marc laboral ha obert, sens dubte, nous horitzons en la problemàtica dels límits del poder de control de l'empresari i, en concret, sobre l'afectació de la dignitat i dels drets fonamentals dels treballadors.

En relació amb l'ocupació d'ordinadors o altres mitjans informàtics de titularitat empresarial per part dels treballadors, es pot afirmar que la utilització d'aquestes eines està generalitzada en el món laboral i correspon a cada empresari, en l'exercici de les seves facultats d'autoorganització, adreça i control, **fixar les condicions d'ús** dels mitjans informàtics assignats a cada treballador.

En el marc d'aquestes facultats de direcció i control empresarials, no hi ha dubte del següent: «Es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales»[35].

[35]STC 241/2012, de 17 de desembre.

En l'àmbit del Consell d'Europa, el Tribunal Europeu de Drets Humans (TEDH) ja ha declarat[36] que la recollida i l'emmagatzematge d'**informació personal** relativa a les trucades telefòniques, correu electrònic i navegació per internet d'una treballadora, sense el seu coneixement, constitueix una **ingerència** en el seu dret al respecte de la seva vida privada i la seva correspondència, en el sentit de l'article 8 del CEDH.

[36]Entre d'altres, a l'STEDH de 3 d'abril del 2007 (assumpte *Copland contra el Regne Unit*) i en la de 25 de juny del 1997 (assumpte *Halford contra el Regne Unit*).

[37]SSTC 114/1984, 175/2000 i 56/2003.

Pel que fa al secret de les comunicacions, el TC ha afirmat, tradicionalment, que la CE garanteix la seva impenetrabilitat per part de tercers, amb la qual cosa rebutja la intercepció o el coneixement antijurídics de les comunicacions alienes[37]. Aquesta última precisió explica que, quan opera, la garantia constitucional es projecti sobre el contingut de la comunicació, tot i que aquest no pertanyi a l'esfera material del que és íntim. Igualment, el TC ha destacat que la noció constitucional de secret de la comunicació cobreix no només el contingut, sinó també altres aspectes d'aquest, com la identitat subjectiva dels interlocutors.

3.1. La doctrina del Tribunal Constitucional sobre la intimitat i el secret de les comunicacions

Cal assenyalar que **el dret a la intimitat s'estén al contingut dels missatges electrònics**, com ja va advertir l'STC 173/2011, de 7 de novembre, en la qual aquest va assenyalar que el cúmul d'informació que emmagatzema el seu titular en un ordinador personal –entre altres, dades sobre la seva vida privada i professional– forma part de l'àmbit de la intimitat constitucionalment protegit; també que l'ordinador és un instrument útil per a l'emissió o recepció de correus electrònics, de manera que pot quedar afectat el dret a la intimitat personal «en la medida en que estos correos o *e-mails*, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado» (FJ 3). No obstant això, sembla que el TC s'aparta d'aquesta doctrina tan clara i nítida en dues resolucions ulteriors: les SSTC 241/2012, de 17 de desembre, i 170/2013, de 7 d'octubre.

1) STC 241/2012

El TC considera que el secret sobre les comunicacions i sobre la intimitat no es veu afectat en un cas en què l'empresa accedeix als fitxers informàtics en què quedaven registrades les converses mantingudes entre dues treballadores per mitjà d'un programa de missatgeria instal·lat per elles mateixes (programa Trillian de missatgeria instantània) sense autorització ni coneixement de l'empresa, en un ordinador d'ús comú i sense clau d'accés (per accedir a la unitat «C»); les converses de caràcter íntim van ser descobertes per casualitat per un treballador, que en va informar a l'empresa, la qual havia prohibit de manera expressa la modificació dels programes informàtics preinstal·lats en els ordinadors. «El TC entiende que no cabe apreciar afectación del derecho a la intimidad desde el momento [en que] fueron ambas trabajadores quienes realizaron actos dispositivos que determinaron la eliminación de la privacidad de sus conversaciones, [al] incluirlas en el disco del ordenador, [en el cual] podían ser leídas por cualquier otro usuario». Així doncs, el seu contingut podia transcendir a terceres persones, com de fet va passar, ja que l'empresa ho sabia perquè un treballador n'havia informat. Pel que fa al secret de les comunicacions, el TC parteix d'un principi de variabilitat de l'abast del poder de vigilància, i afirma que els graus d'intensitat o rigidesa amb què han de ser valorades les mesures empresarials de vigilància i control són variables «en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin».

D'aquesta manera, «la posibilidad de uso común del ordenador por todos los empleados permite considerar que la información archivada en el disco duro era accesible a todos los trabajadores, sin necesidad de clave de acceso alguna». Aquesta disposició organitzativa d'ús comú permet afirmar la seva incompatibilitat amb els usos personals i reconèixer que, en aquest cas, la pretensió de secret no té cobertura constitucional, ja que falten les condicions necessàries

per a la seva preservació. El TC considera que les comunicacions dels treballadors queden fora de la protecció constitucional del secret de les comunicacions, ja que la sentència diu això de les formes d'enviament: «Se configuran legalmente como comunicación abierta, esto es, no secreta».

2) STC 170/2013

L'Alt Tribunal considera que

> «basta que un convenio colectivo sancione/prohíba el uso de herramientas informáticas y correo electrónico para usos diversos al profesional, para considerar que la empresa puede controlar los correos electrónicos de los empleados[38], sin aviso previo a estos y sin que ello vulnere su derecho al secreto de las comunicaciones y el derecho a la intimidad».

(38)Ex arts. 5.a, 20.2 i 20.3 ET.

La sentència acull la tesi de l'empresa demandada en el sentit que el context normatiu –el conveni col·lectiu– permetia saber al treballador la prohibició d'un ús no professional del correu electrònic, així com la possibilitat que l'empresari accedís al seu contingut per vigilar la seva correcta utilització. Per aquesta raó, entén que, encara que l'empresa no hagués protocol·litzat una política corporativa en aquest sentit, «la prohibición establecida en el convenio[39] impide que el trabajador pudiera albergar una razonable expectativa de reserva o confidencialidad de sus mensajes enviados o recibidos a través de dicho medio», configurado por tanto como un «canal abierto» a la inspección y control empresarial, por lo que «no se vulnera el derecho al secreto de las comunicaciones ajenas».

(39)En el cas analitzat pel TC, l'article 79.2 CC de la indústria química assenyala que el correu electrònic és d'«exclusiu ús professional».

A manera de tancament, la doctrina del TCO exigeix que els mitjans de control de l'activitat laboral per part de les empreses **siguin justificats, idonis, necessaris i proporcionats** per evitar la lesió dels drets fonamentals del treballador, com intimitat, honor, pròpia imatge o dignitat[40].

(40)SSTCO 186/2000, 98/2000, 292/1993, 99/1994, 106/1995 o 136/1996.

D'aquesta manera, «la prohibición del control oculto[41], encuentra una excepción específica, que queda referida a que ese control sea la única forma posible de satisfacer el interés empresarial».

(41)Cal advertir els treballadors de la mesura concreta de vigilància i control que s'adoptarà per verificar el compliment de les obligacions laborals.

(42)STC 186/2000.

«Se admite el control oculto en los casos en que se tenga la sospecha de que el trabajador está cometiendo un ilícito grave, como puede ser la apropiación de dinero o de bienes de la empresa[42], [si bien] no basta la mera sospecha de que el trabajador esté incurriendo en un ilícito». No obstant això, la validesa del mitjà de control utilitzat requereix que aquest compleixi dos criteris, en concret, que l'interès empresarial a controlar l'activitat del seu empleat estigui prou justificat i no es basi en una simple conveniència de l'empresari i que hi hagi indicis raonables sobre l'incompliment d'obligacions o deures laborals per part del treballador «controlat» (judici d'idoneïtat, de necessitat i de proporcionalitat[43]).

[(43)]STC 96/2012.

3.2. La doctrina del Tribunal Suprem sobre la intimitat i el secret de les comunicacions

L'**STS 2007.09.26** (u. d. 966/2006) analitza la prova il·lícita obtinguda amb el registre d'un ordinador: director general d'una empresa, que prestava serveis en un despatx sense clau, en què disposava d'un ordinador que no té clau d'accés i connectat a la xarxa de l'empresa mitjançant ADSL; quan el tècnic d'una empresa d'informàtica va ser cridat per comprovar els errors de l'ordinador, va detectar l'existència de virus informàtics, com a conseqüència de «la navegació per pàgines poc segures d'internet»; davant aquest cas, s'assenyalen les cinc premisses a l'efecte:

1) El control de l'ús de l'ordinador facilitat al treballador per l'empresari no es regula per l'article 18 de l'ET, sinó per l'article 20.3 de l'Estatut dels treballadors.

2) Les comunicacions telefòniques i el correu electrònic estan inclosos en l'àmbit de la intimitat i en la protecció addicional que deriva de la garantia constitucional del secret de les comunicacions, de manera que entren dins de la garantia de tutela de la intimitat dels arxius personals del treballador que es trobin a l'ordinador i també entra en aquesta tutela l'historial de navegació per internet.

3) No és obstacle per a la protecció de la intimitat que l'ordinador **no tingués clau d'accés**, ja que aquesta dada no suposa per si mateixa una acceptació per part del treballador d'un accés obert a la informació continguda al seu ordinador.

4) Hi ha un **hàbit social generalitzat de tolerància** amb certs usos personals moderats dels mitjans informàtics i de comunicació facilitats per l'empresa als treballadors, de manera que aquesta tolerància crea una expectativa també

general de confidencialitat en aquests usos (expectativa que no pot ser desconeguda, tot i que tampoc pot convertir-se en un impediment permanent del control empresarial).

5) L'empresa, d'acord amb les exigències de bona fe, ha d'establir prèviament les **regles d'ús d'aquests mitjans** –amb aplicació de prohibicions absolutes o parcials– i informar els treballadors que els controlaran i amb quin mitjans comprovaran la correcció dels usos, així com de les mesures que s'han d'adoptar en el seu cas per garantir l'efectiva utilització laboral del mitjà quan calgui, sense perjudici de la possible aplicació d'altres mesures de caràcter preventiu, com l'exclusió de determinades connexions (d'aquesta manera, si el mitjà s'utilitza per a usos privats en contra d'aquestes prohibicions i amb coneixement dels controls i mesures aplicables, no podrà entendre que, en realitzar el control, s'ha vulnerat «una expectativa raonable d'intimitat»).

L'**STS 8.3.2011** (u. d. 1826/2010) declara la nul·litat de la prova obtinguda mitjançant una auditoria informàtica que tenia la finalitat de revisar la seguretat del sistema i detectar possibles anomalies en la utilització dels mitjans posats a disposició dels empleats. La sentència declara il·lícita la prova obtinguda d'aquesta manera perquè no consta que, d'acord amb les exigències de la bona fe, l'empresa hagués establert prèviament **algun tipus de regles per a l'ús d'aquests mitjans** –amb aplicació de prohibicions absolutes o parcials–, ni tampoc que s'hagués informat els treballadors que es faria un **control** ni dels mitjans que s'aplicarien per a comprovar que se'n feia un ús adequat.

L'evolució de la doctrina anterior s'acompanya de l'**STS 2011.10.06** (u. d. 4053/2010), que indica que el més important, admesa la facultat de control de l'empresari i la **licitud d'una prohibició absoluta dels usos personals**, consisteix a determinar si hi ha o no un dret del treballador que es respecti la seva intimitat quan, en contra de la prohibició de l'empresari o amb un advertiment exprés o implícit de control, utilitza l'ordinador per a fins personals. La resposta sembla clara:

> «Si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque, al no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo».

Per la seva banda, l'Agència Espanyola de Protecció de Dades, en el seu informe 0247/2008, indica que l'article 20.3 ET **habilita l'ocupador** a controlar l'ús d'aquests instruments (ordinadors), però sempre que prèviament hagi informat el treballador d'aquest extrem. És a dir, com es diu a l'STSJ Madrid 2015.10.04 (Regl. 57/2015), STS 8.3.2011 (u. d. 1826/2010).

> «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 para 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.»

Així doncs, alguns pronunciaments recents[44] han reconegut la procedència de l'**acomiadament disciplinari** (transgressió de la bona fe contractual i abús de confiança) per la inadequada utilització, per part d'una treballadora, de les eines informàtiques disposades per l'empresa per al correcte desenvolupament de la seva activitat professional, quan hi havia normes de prohibició conegudes pels treballadors:

(44)STSJ Catalunya 2016.06.13 (Regl. 2131/2016).

> «La cuenta de correo electrónico era para el uso exclusivo de tareas profesionales en la empresa, pudiendo ser auditada en cualquier momento[45], y se prohibía terminantemente enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sobre productos o servicios; utilizar la red para promover el acoso sexual, juegos de azar, sorteos, subastas, descargas de vídeo o audio y cualquier otro material no relacionado con la actividad profesional, o utilizar de forma abusiva o incontrolada los recursos telemáticos de la empresa, incluida la red internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo de cada usuario».

(45)Que, un cop realitzada, va ser la que va motivar l'acomiadament.

La treballadora, malgrat tot, es va connectar a internet des de l'ordinador de l'empresa per consultar el seu correu electrònic particular, jugar al parxís i consultar el seu perfil en xarxes socials durant un total d'1 hora i 52 minuts; altres cops es va connectar a internet des de l'ordinador de l'empresa per consultar el seu correu electrònic particular, jugar al parxís, consultar el seu perfil en xarxes socials i consultar pàgines de venda de mobiliari, durant un total d'1 hora i 3 minuts; i en una tercera ocasió, es va connectar a internet des de l'ordinador de l'empresa per consultar el seu correu electrònic particular, jugar al parxís, consultar el seu perfil en xarxes socials i consultar pàgines de venda de mobiliari, viatges i telefonia durant un total de 27 hores i 5 minuts.

En sentit similar, l'**STSJ Madrid 2015.01.26** (Regl. 679/2014) declara la procedència de l'acomiadament disciplinari, a propòsit d'un empleat de l'empresa INDRA SISTEMAS que, vulnerant la prohibició absoluta (clàusula desena del contracte de treball, codi de conducta corporatiu i manual general) d'ús d'ordinadors i accés a internet (cada treballador té la seva contrasenya privada i personal) per a fins aliens a l'activitat de l'empresa, i va accedir, en un marc temporal de dos mesos, durant 16 hores i 47 minuts el mes d'octubre del 2013 (vint-i-un dies laborables) i 10 hores 43 minuts el mes de novembre del 2013 (setze dies laborables) a nombroses pàgines web de contingut no professional, que, entre altres, inclouen xarxes socials (Facebook, Twitter), serveis de correu electrònic personal (hotmail.com) i pàgines web de compres i/o moda (elcorteingles.es, zara.net, entre altres).

3.3. Control del correu electrònic, de la navegació web i ús «irregular» per part de l'empleat

Com a regla general, si hi ha ús compartit dels mitjans de treball o amb lliure accés de tercers conegut pel treballador (el que s'anomena «comunicació oberta»), l'ús «privat» (no laboral) d'aquests dispositius per part del treballador per l'accés a internet suposa un risc consentit i conscient que l'empresa o terceres persones **puguin accedir a aquesta informació**, el que es coneix com a «troballa casual», i, per això, sense perpetrar un atemptat contra la seva intimitat[46].

(46)STC 170/2013, de 7 d'octubre.

No obstant això, com ha assenyalat l'STS de 2007.09.26 (u. d. 966/2006), es vulnera el dret a la intimitat del treballador quan, tot i que l'entrada inicial a l'ordinador d'un treballador podia justificar-se per l'«existència d'un virus», l'actuació empresarial lligada no es va aturar en les tasques de detecció i reparació, sinó que «se siguió con el examen del ordenador para entrar y apoderarse de un archivo cuyo examen o control no podía considerarse que fuera necesario para realizar la reparación interesada», ja que aquest professional no és proporcional.

En el cas del **control del correu electrònic**, l'ús del correu per part del treballador està emparat «por el derecho a la intimidad en relación con la información allí contenida» (safates d'«entrada» i «sortida») i per la seva connexió amb el dret al secret de les comunicacions (art. 18.3 CE). Com indica l'STC 142/2012, de 2 de juliol:

> «El derecho al secreto de las comunicaciones consagra la interdicción de la interceptación o del conocimiento antijurídico de las comunicaciones ajenas, por lo que dicho derecho puede resultar vulnerado tanto por la interceptación, en sentido estricto, consistente en la aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o la captación del proceso de comunicación, como por el simple conocimiento antijurídico de lo comunicado a través de la apertura de la correspondencia ajena guardada por su destinatario o de un mensaje emitido por correo electrónico o a través de telefonía móvil, por ejemplo».

En relació amb la **navegació per internet a pàgines web no relacionades amb la feina**, s'ha escrit i comentat molt. Resumidament, n'hi ha prou a dir:

a) El treballador no es troba emparat pel dret al secret de les comunicacions perquè no s'està realitzant una comunicació amb un altre, sinó buscant informació o realitzant qualsevol altra gestió en línia a títol no laboral, ni tan sols quan estigui en un xat o en un fòrum si aquest és de lliure accés.

b) Sí es troba emparat pel dret a la intimitat, ja que la connexió a aquestes pàgines **pot revelar informació privada o sensible del treballador**, atès que el seu rastre queda registrat en els arxius temporals de l'ordinador (*cookies*).

c) La implantació de protocols d'actuació, instruccions a la intraweb, codis de conducta/bones pràctiques i ús responsable dels equips de treball posats a disposició del treballador, a manera de «condicions d'ús», i fins i tot l'exclusió d'accés (*firewalls*), si són conegudes pels treballadors[47], permeten el control i la sanció empresarial d'un ús prohibit, abusiu (més enllà d'un de singular, ocasional i/o justificat ús «personal», per exemple, una urgència familiar) o indegut[48].

(47)Via CC (STC 170/2013), manual (STSJ Madrid 2012.12.19 –Regl. 3149/2012–) o com a annex al contracte de treball (Informe AEPD 464/2013).

(48)STC 241/2012.

D'aquesta forma, com indica la STSJ d'Astúries de 30 de gener del 2015 (Rº 28/2015), no existeix vulneració del dret a la intimitat pel registre de l'ordinador del treballador si estava prohibit l'ús dels recursos telemàtics de l'empresa per a activitats no relacionades amb el lloc de treball i si el treballador havia signat un document de confidencialitat en què l'empresa es reserva el dret de revisar, sense avís previ, els missatges de correu electrònic. Per descomptat, l'accés d'un treballador a l'ordinador del seu superior, mitjançant l'ús de les seves contrasenyes, per a copiar en una unitat externa USB determinats documents i correus electrònics, que posteriorment va obrir després de traspassar-los al seu ordinador, sense que s'apliquin les garanties de l'article 18 ET per a consultar el contingut de l'ordinador del treballador acomiadat[49], és una prova obtinguda de forma il·lícita.

(49)STSJ de Catalunya de 7 de novembre del 2014 (Rº 4585/2014).

Un altre cas d'interès és el recollit per l'**STSJ Extremadura 2014.12.17** (Regl. 543/2014) a propòsit de l'acomiadament, declarat procedent, d'un empleat –cap de manteniment d'un hotel– que va utilitzar l'ordinador de l'empresa per accedir a internet amb fins particulars durant la jornada laboral (pàgines pornogràfiques –una mitjana de 2 hores diàries–, Facebook, YouTube i HTTP Browsing), de manera que va contravenir les ordres de l'empresa (prohibició absoluta d'ús no laboral de l'ordinador).

En síntesi: un acomiadament (disciplinari) o sanció és apropiat quan l'ús d'internet o correu electrònic per a fins no laborals suposi danys a l'empresa (per exemple, descàrrega de virus, col·lapse del servidor[50]), o quan l'«ús indegut» afecti la prestació laboral o al «clima» laboral amb els companys de treball (remissions massives de correus electrònics amb continguts ofensius, assetjament) o quan s'hi accedeixi després de sortejar el tallafoc o després d'incomplir protocols de seguretat[51], o, finalment, quan s'intenti modificar l'adreça IP amb formateig del disc dur i deshabilitació de programes, si l'empresa ha avisat prèviament de la instal·lació d'un programa de control per comptabilitzar el temps que cada treballador utilitza a internet, sense afectar el contingut del correu electrònic[52].

(50)STSJ Catalunya 31.03.2012 (R 5955/2011).

(51)STSJ Astúries 2013.10.15 (Regl. 1575/2013).

(52)STSJ Comunitat Valenciana 5.10.2010 (Regl. 2195/2010).

També resulta de gran interès la consulta de l'**STSJ País Basc de 2015.09.29** (Regl. 1245/2015), la qual resol el cas d'un empleat (**acomiadament procedent**) que navegava per internet per a fins particulars aliens a la feina, tot i

la prohibició absoluta fixada per l'empresa, accedeix al perfil personal d'un altre company mitjançant el servidor d'un client per control remot, navega pel servidor del client sense que la seva activitat es vegi reflectida al part diari i intenta sabotejar el sistema de control d'activitat (l'empresa havia col·locat un programa «espia» que remet fotografies de la pantalla de l'ordinador per mitjà d'un correu electrònic a una adreça). El programa espia en qüestió s'anomena NTKlauss i va ser notificat als treballadors com a forma de control de la seva activitat, el qual reporta un informe d'activitat cada minut per treballador, que porta signatura digital d'autenticitat relacionada amb l'usuari corresponent i que s'envia per correu electrònic al departament de personal. Al seu torn, en executar el control remot d'un client, cada cinc minuts el programa feia una foto del que apareixia a la pantalla de l'ordinador i l'enviava per correu electrònic amb signatura digital i, finalment, detectava els atacs al programa o qualsevol manipulació mitjançant un sistema de control ocult que enviava foto i alerta en temps real amb signatura digital (certificada per la mercantil NTS) de l'activitat que es desenvolupa.

Resumidament, i com a colofó: segons l'**STC 170/2013**, de 7 d'octubre, no hi ha vulneració del dret fonamental al secret de les comunicacions, en l'àmbit de les relacions laborals, per l'accés de l'empresa als fitxers informàtics en què quedaven registrats els correus privats del treballador, ja que es va produir un incompliment de la prohibició expressa de l'ús extralaboral que portava implícita la facultat de l'empresa de controlar la seva utilització; mentre que, segons l'STEDH 2016.01.12 (assumpte *Barbulescu*), una empresa pot controlar els missatges dels seus treballadors en un servei de missatgeria instantània professional per internet sempre que prèviament hagi prohibit de manera expressa l'ús dels mitjans de comunicació de l'empresa (Yahoo Messenger) per a fins personals.

De totes maneres, una altra lectura de la qüestió és possible. Em refereixo al fet que, com assenyala el vot particular de l'**STSJ Castella i Lleó de 2012.12.05** (Regl. 1691/2012), en un cas en què una treballadora va visitar, en més d'un 70%, pàgines extralaborals durant la seva jornada laboral malgrat la prohibició expressa de l'empresa, de manera que la sala va declarar la procedència de l'acomiadament. Indica el vot particular que:

«No consta sin embargo cuál fuese el tiempo que la trabajadora dedicó a tales actividades extralaborales, ni la incidencia en su productividad, ni siquiera el número de accesos extralaborales (solamente figura el porcentaje, así como la media estadística en la empresa en esos dos meses, que fue de 60.000 por persona). Lo cierto es que estamos realmente ante un despido "estadístico", según resulta claramente de los hechos probados. La empresa realiza un estudio de consumo del ancho de banda en los meses de octubre y noviembre de 2011 y procede a despedir a aquellos trabajadores cuyos accesos a páginas web de internet exceden notablemente de la media. Analizado el caso de la trabajadora, lo único que se determina es que había visitado páginas web extralaborales, conociendo solamente el porcentaje de distribución entre accesos extralaborales (70 %) y laborales (30 %). Nada más sabemos, como digo, respecto de la incidencia de tal dedicación extralaboral en el tiempo de trabajo, rendimiento o productividad».

La didàctica del vot particular esmentat és formidable:

> «[…] determinadas órdenes empresariales serían ilícitas en principio, salvo que se justificasen de forma proporcionada y suficiente por las necesidades específicas de la organización productiva […] si la empresa proporciona al trabajador de un ordenador u otro dispositivo con conexión abierta para la navegación web, no puede estimarse ilegítimo que el trabajador pueda acceder a alguna web extralaboral, con las mismas limitaciones antedichas (siempre que no descuide indebidamente su dedicación laboral, esto es, la falta de rendimiento ya analizada anteriormente) e incluso en tales condiciones sería ilegítima en principio una orden empresarial prohibiendo tal acceso […]. Obviamente, la empresa puede establecer prohibiciones y límites ajustados y proporcionados, siempre que acredite motivos legítimos para los mismos (por ejemplo, por razón de reservar suficiente ancho de banda), pero en tal caso la prohibición debe ser ajustada a tales necesidades. Y, obviamente, puede modificar la organización productiva para mejorar el rendimiento o ajustarla mejor a sus necesidades (por ejemplo, proporcionando un vehículo al cartero para que haga su trabajo más rápido y con menores distracciones, o limitando los accesos posibles a unos sitios web determinados). […] Entiendo que admitir por el órgano judicial la licitud de una orden de prohibición absoluta, desconectada de sus finalidades productivas legítimas, así como la máxima sanción incondicionada para su incumplimiento, supone una interpretación irracional y desproporcionada de las normas jurídicas aplicables vulneradora del artículo 24.1 CE».

En definitiva: prohibició d'ús extralaboral d'internet/correu electrònic sí, però **proporcionat i connex a la finalitat productiva**, no de qualsevol manera i sense una mínima explicació de les raons per les quals es du a terme.

El TEDH ha tingut ocasió de pronunciar-se sobre el control del correu electrònic i/o la navegació dels empleats per internet, a propòsit de l'article 5 CEDH (respecte a la vida privada i familiar). En concret, primer s'hi va pronunciar amb la STEDH de 12 de gener del 2016 (assumpte *Barbulescu-I*), on indicava que els correus electrònics enviats des del lloc de treball i la informació recollida per mitjà d'una vigilància de l'accés a internet per a fins personals ha de rebre la protecció de l'article 8 CEDH com a part de la noció de «vida privada» i «correspondència», igual que queden incloses les trucades telefòniques des del lloc de treball. De la mateixa manera, fa al·lusió a l'expectativa raonable de privacitat que existeix quant al correu i a l'ús del web. El TEDH arriba a la conclusió que, donada la prohibició total de l'empresa sobre l'ús amb fins personals de recursos electrònics posats a disposició dels empleats (Yahoo Messenger, en aquest cas), l'empresari havia actuat de manera legítima (comiat disciplinari del treballador) a l'hora de comprovar si l'empleat estava duent a terme tasques professionals durant el seu horari laboral, i assenyala que és raonable que l'empleador vulgui verificar que els seus empleats estan efectivament complint les seves funcions i tasques durant l'horari de treball, ja que «el monitoreo del empleador tiene un alcance limitado y respeta el principio de proporcionalidad».

No obstant això, revisant la seva pròpia doctrina via recurs, la STEDH de 5 de setembre del 2017 (assumpte *Barbulescu-II*) ha indicat 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 prohibían

su utilización con fines personales». Per això, assenyala quins són els criteris que ha de seguir un tribunal nacional per a ponderar si el control empresarial és correcte o no:

> «a) l'existència de notificació a l'empleat de la possibilitat d'adoptar mesures de vigilància electrònica i la seva implementació;
>
> b) l'abast i el grau d'intrusió en la privacitat de l'empleat per l'esmentada vigilància electrònica;
>
> c) l'existència i la comunicació de raons legítimes per a justificar la vigilància i l'accés a continguts específics com a conseqüència directa d'aquest monitoratge;
>
> d) l'existència de mesures menys intrusives [d'acord amb el principi de necessitat];
>
> e) les conseqüències de l'esmentada vigilància electrònica per al treballador i el potencial ús per part de l'empresa dels continguts adquirits mitjançant aquesta vigilància;
>
> f) l'existència de garanties adequades, sobretot quan les operacions de vigilància són intrusives».

En resum: de la doctrina del TEDH es pot entendre que es reconeix, de manera expressa, la legitimitat i la validesa de la vigilància electrònica en el context laboral, però aquest poder de l'empresari està subjecte a garantir els drets (intimitat, vida privada i protecció de dades) dels treballadors, assegurant que els principis de transparència, necessitat i proporcionalitat siguin respectats i «se lleven a cabo políticas laborales que tengan en cuenta el aviso previo al control o vigilancia».

La STS de 17 de març del 2017 (rec. 55/2015) també ha assenyalat la importància per a les empreses de «contar con unas normas de uso de los medios informáticos preestablecidas», per tal d'assegurar el valor probatori dels correus electrònics derivats d'una ingerència empresarial en el compte de correu electrònic professional d'un empleat.

3.4. Sobre la utilització d'imatges o vídeos «penjats» a Facebook (o altres xarxes socials) per sancionar el treballador

Un bon exemple de l'**acomiadament derivat de vídeos obtinguts del perfil de Facebook** i penjats per la treballadora, de manera que fossin accessibles a tercers, el trobem en l'**STSJ de Castella i Lleó de 2014.04.30 (Regl. 491/2014)**. S'hi relata que una treballadora va penjar al seu perfil de Facebook dos vídeos obtinguts de la càmera de seguretat de la botiga on prestava serveis com a encarregada, en els quals es veu la caiguda a terra de dues caixeres, fet que va provocar comentaris jocosos d'altres usuaris. Va ser acomiadada per aquesta conducta, mesura que el Jutjat Social va qualificar de procedent. En suplicació, la treballadora denuncia que la decisió judicial es basa en una prova obtinguda amb vulneració del seu dret fonamental a la protecció de les dades personals. La sentència desestima el recurs, en el qual s'argumenta: «las imágenes no eran propiedad de la actora, sino de la empresa, y la demandante las difundió

en una red social accesible posibilitando así que las viesen una pluralidad de personas» (alguna de les quals les va fer arribar a l'empresa). Això va perjudicar el dret a l'honor i a la intimitat de les seves companyes.

En aquest sentit, l'**STSJ d'Astúries de 2013.06.14** (JUR 2013\245751) declara procedent l'acomiadament d'una treballadora amb baixa mèdica per contractura cervical que, l'endemà d'iniciar el procés d'IT, va viatjar a Madrid amb avió i va estar amb unes amigues en un parc d'atraccions i en dos dies va estar en diversos bars fins a altes hores de la matinada. L'acomiadament es procedent perquè la conducta de la treballadora mostrava aptitud laboral per a l'exercici de les comeses pròpies de la seva professió de cambrera. En aquest cas, s'al·lega la violació de l'article 18.3 de la Constitució per la causa següent: «La prueba de los hechos que se imputan a la trabajadora a través de páginas de redes sociales (Facebook)»; però, el TSJ d'Astúries considera que no s'ha vulnerat la intimitat de la treballadora, «al haber sido obtenidas las fotografías sin necesidad de utilizar clave ni contraseña alguna para acceder a ellas, dado que no estaba limitado el acceso al público, de modo que se obtuvieron libremente, pues al estar "colgadas" en la red, pudieron ser vistas sin ningún tipo de limitación», de manera que no hi ha una intromissió en la intimitat de la treballadora, que, a més apareix en les instal·lacions d'un parc d'atraccions de Madrid (per tant, en un lloc públic).

La **publicació de fotografies a les xarxes socials**, que acrediten la realització d'activitats que anirien en contra d'una incapacitat temporal concedida a un treballador, no està protegida pel dret a la intimitat, llevat que es configuri d'aquesta manera que hi hagi una restricció als continguts publicats per mitjà de claus o contrasenyes.

En el cas de l'**STSJ Andalusia-Sevilla 2015.10.29** (Regl. 2723/2014), es declara la procedència d'un acomiadament disciplinari a propòsit de «viatges d'oci» d'una treballadora dedicada a la recol·lecció de taronges en situació d'IT, que reflecteixen, per fotos a Facebook, que realitza activitats lúdiques incompatibles amb el seu estat de salut, i després d'haver penjat també la treballadora al seu compte públic de Facebook (conegut com a «mur») altres «floretes» com les següents (fets provats de la sentència):

> «[...] fotografía de una naranja, respecto de la cual se vertía una serie de comentarios por interlocutores de la actora tales como: "¡Parece un consolador anal!"; "qué naranjos más raros tenéis ¿no? O ¿ya lo sembráis así para sacarles provecho?", a lo que la actora insertó el siguiente comentario: "Estos son raros como los jefes"; o se encontraba colgada una foto de empleados de las demandadas [...] y un comentario insertado por la actora que decía: "estos son los ex compañeros de trabajo, o sea, los hijos de puta"».

Així doncs, el control empresarial pot estendre fins i tot fins a buscar fotos i informació dels seus treballadors en situació d'incapacitat temporal en xarxes socials (STSJ de Canàries-Las Palmas 2016.01.22 –Regl. 1167/2015).

Altres casos d'interès mereixen ser portats a col·lació:

1) STSJ Galícia 2014.10.08 (Regl. 2941/2014)

Es considera procedent l'acomiadament d'un treballador (especialista de manteniment) que presta serveis a la casa sacerdotal de la diòcesi d'Ourense i publica a Facebook expressions injurioses, denuncia haver estat víctima d'humiliacions, amenaces i enganys per ser «negre i immigrant», afirma que «condemnen l'homosexualisme i entre els seus jerarques hi ha pedòfils» i es refereix a «la perversió d'aquesta religió», al fet que «viuen de les dones i altres se'n van de prostitutes que jo els he vist», al fet que «és immoral i il·legal això que fa l'Església catòlica romana».

Respecte a aquestes expressions, la Sala de suplicació indica que

> «es evidente que la libertad de expresión ampara la crítica, pero no las injurias ni, mucho menos, comportamientos que bien pudieran integrarse en la calumnia; porque lo que el (trabajador) hace es faltar al respeto debido a su empleadora, lanzando unas duras acusaciones, genéricas invectivas, que lo único que tratan es desprestigiarla y vulnerar su imagen de cara al público. […] No es de recibo, además, que se pretendan justificar esas expresiones en la existencia de gravísimos y repugnantes delitos (pedofilia), por todos conocidos, cometidos en ocasiones por sacerdotes; ni en un folclore que es rico en toda clase de estereotipos, que nada tienen que ver con unas rechazables ofensas; y, por otra parte, el ánimo del actor no era –empleando una terminología penal– *iocandi* –que es la propia del ingenio popular–, sino *iniuriandi* directamente; aparte de que en su «muro» no colgó un dicho, un refrán, un aforismo o una canción, sino afrentas o imputaciones atentatorias contra el buen nombre de su empresaria».

2) STSJ Aragó 2016.05.18 (Regl. 300/2016)

Es declara la procedència de l'acomiadament d'un treballador per missatge vexatori i ofensiu contra els seus superiors jeràrquics, companys de feina i tercers penjat al Facebook i després visibilitzat mitjançant «captures de pantalla» via WhatsApp entre els companys d'una treballadora (infermera). A la sentència es planteja si el caràcter tancat del compte de Facebook podria vulnerar el dret al secret de les comunicacions i de la intimitat de la treballadora. Respecte al primer, el tribunal va considerar que el fet que els destinataris del missatge fossin només alguns amics

> «en modo alguno excluye que estos, como sucede habitualmente en las redes sociales, divulguen posteriormente esta información, que la empresa no conoce porque haya interceptado comunicaciones ajenas, ni porque haya accedido antijurídicamente a su contenido, sino porque la difusión de esa información por sus destinatarios llegó a la supervisora de la accionante».

Respecte al segon, s'argumenta que el respecte a la intimitat de la treballadora no pot emparar una conducta consistent a «insultar gravemente a otros trabajadores, a sabiendas de la difusión que habitualmente tienen estos comentarios en estas redes».

3) STSJ Catalunya 2016.03.03 (Regl. 191/2016)

En un assumpte en el qual un treballador (cantant de la Fundació Gran Teatre del Liceu) va realitzar un seguit de manifestacions a la pàgina de Facebook contra l'empresa (va qualificar de «corruptes» i «mafiosos» el director del cor del teatre –a qui també imputa «tracte de favor» en la contractació d'altres persones–, el director de l'orquestra i el director de recursos humans, del qual va denunciar l'«opacitat» dels seus salaris), entén que no s'han superat els límits de la llibertat d'expressió, ja que no suposen «injúria», sinó «simple ànim de crítica o denúncia», encara que siguin «exagerades, desagradables i sobretot poc afortunades i sens dubte reprotxables moralment»; llibertat d'expressió que empara una persona a la qual

> «le han negado varias veces su reincorporación a su anterior puesto de trabajo desde su situación de excedencia, a quien ve como se contrata a otras personas sin aparente justificación, o a quien según parece y a su juicio no cumple con los mínimos de trasparencia e integridad que como empresa que se nutre de fondos públicos corresponde, etcétera».

4. La videovigilància al lloc de treball

Els enregistraments mitjançant càmeres de vídeo i els enregistraments d'àudio han estat, a la pràctica, els casos més habituals que han hagut d'analitzar els tribunals de justícia en el context laboral. Moltes vegades, tots dos conflueixen en un sol mitjà (gravacions de vídeo amb àudio). Pel que fa al dret fonamental afectat, la videovigilància afecta o sol afectar la intimitat del treballador (art. 18.1 CE), o fins i tot el dret a la pròpia imatge (art. 18.1 CE) –STC 99/1994, «deshuesador de jamón»–; mentre que els enregistraments en àudio poden incidir no només –i amb més intensitat– en la intimitat, sinó també en l'àmbit del secret de les comunicacions (art. 18.3 CE) quan l'enregistrament d'àudio té per objecte el contingut d'una comunicació. A més a més, l'habitualitat de les videoconferències (Skype, etc.) com a mitjà de comunicació fa que també els enregistraments de vídeo i àudio en què aquestes consisteixen no es trobin només emparats pel dret a la intimitat, sinó també pel secret de les comunicacions.

D'altra banda, el dret a la protecció de dades de caràcter personal (art. 18.4 CE, LO 15/1999) també es pot veure afectat per aquest tipus de mesures[53], des del moment en què les imatges gravades en un suport físic constitueixen una dada de caràcter personal que queda integrada en la cobertura de l'article 18.4 CE. En aquest sentit, l'STC 29/2013 afirma que

(53)SSTCO 292/2000 i 29/2013.

> «no contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo».

L'enregistrament d'imatges en càmera de vídeo instal·lada al centre de treball pot ser una mesurada idònia, necessària i equilibrada al fi pretès de provar un determinat incompliment laboral d'un treballador en el seu lloc de treball que, per això, sigui després sancionat disciplinàriament[54], però això és així, com a regla general, quan els treballadors (i ja no diguem els seus representants) tenen **coneixement previ** de la instal·lació de càmeres de vigilància i de la finalitat i utilitat d'aquestes càmeres, però no quan aquesta instal·lació sigui la base per, a partir de càmeres destinades a un ús genèric com el control d'accessos, realitzar un control de l'activitat laboral (en aquest sentit, a propòsit del compliment de la jornada laboral, STC 29/2013, d'11 de febrer).

(54)A tall d'exemple, SSTSJ Catalunya 2013.07.01 (Regl. 1804/2013).

Els requisits perquè les proves obtingudes mitjançant enregistraments d'àudio o vídeo (o ambdos) siguin lícites són:

- Que s'obtinguin en l'exercici regular dels poders de vigilància i control. Per això, «no se consideran idóneas las medidas de videovigilancia instaladas en lugares de la empresa donde no se desarrolla la relación laboral», com als lavabos, vestuaris, dutxes, menjadors, etc. Així, les proves obtingudes de la filmació d'aquests llocs s'han de considerar, en principi, il·lícites; ara bé, s'ha considerat lícit posar controls a les portes dels lavabos, sempre que no es visualitzi l'interior[55].

(55)STS, Sala Penal, 1998.07.07 (RJ 1998/5830).

- Que es trobin destinades a verificar el compliment per part del treballador de les seves obligacions i deures. Per això, es considera que la gravació indiscriminada de veu és desproporcionada, perquè és una intromissió més greu en la intimitat que la de la imatge i perquè la gravació de converses entre treballadors o entre aquests i clients no es justifica per la verificació del compliment per part del treballador de les seves obligacions o deures[56]. Això té les seves excepcions, precisament en casos com el telemàrqueting, en què el treball es realitza exclusivament per mitjà de converses telefòniques amb clients[57].

(56)STC 98/2000.

(57)STS 2003.12.05 (RJ 2004/313).

- Que s'informi prèviament al treballador de la possibilitat que es captin imatges o so amb la finalitat de controlar l'activitat laboral i que les imatges o el so captats no s'utilitzin per a finalitats diferents d'aquelles per a les quals el treballador ha estat informat: hi ha un deure d'informació que protegeix enfront d'intromissions il·legítimes en la intimitat[58]. L'informe previ al treballador (o l'empresari) haurà de ser excepcionat en els casos d'indicis raonables de realització d'actes contraris a la bona fe contractual que puguin merèixer sanció d'acomiadament o extinció del contracte pel treballador, i en què l'enregistrament de vídeo no tingui vocació de permanència (temps estrictament necessari), sinó que sigui l'únic mitjà que serveixi per provar la conducta del treballador o de l'empresari (per exemple, supòsits d'assetjament laboral o de sostracció de diners de l'empresa).

(58)STC 196/2004, de 15 de novembre.

- Que es respectin la dignitat i els drets fonamentals del treballador, i les mesures de vídeo o audiocontrol estaran subjectes al test de proporcionalitat, per la qual cosa cal constatar si compleixen els tres requisits o condicions següents: judici d'idoneïtat (si aquesta mesura és susceptible d'aconseguir l'objectiu proposat), judici de necessitat (si, a més, és necessària, en el sentit que no hi hagi una altra mesura més moderada per a la consecució d'aquest propòsit amb la mateixa eficàcia) i judici de proporcionalitat en sentit estricte (si la mesura és ponderada o equilibrada, ja que se'n deriven més beneficis o avantatges per a l'interès general que perjudicis sobre altres béns o valors en conflicte).

Exemples del que s'ha descrit fins ara no en falten: per exemple, la videovigilància supera el test de proporcionalitat (lícita) quan «recogen el uso lúdico por el trabajador de las instalaciones de la empresa»[59] o quan «la grabación se limita a la zona de trabajo, caja registradora, almacenamiento de productos y rebotica, donde lógicamente podían cometerse las supuestas irregularidades y comprobar si se trataba de un hecho aislado, de un error o de una conducta reiterada»[60]. No obstant això, no supera aquest test, per exemple, quan «del contenido de las grabaciones se constata que las imágenes tomadas (microcámaras ocultas, bajo las mesas de las trabajadoras y en el marco de la puerta del aseo utilizado por aquellas) corresponden a las piernas y ropa interior de varias trabajadoras, así como a los órganos genitales femeninos»[61], o quan s'instal·la una «cámara de videovigilancia en taquilla de venta de billetes que realiza una grabación permanente de la zona en la que se encuentran el perchero con la ropa del trabajador y el lavabo»[62].

(59)STSJ País Basc 19.6.2007 (AS 2007/3357).

(60)STSJ Extremadura 2008.01.29 (AS 2008/951).

(61)STSJ Astúries 2003.09.05 (JUR 2003/229062).

(62)STSJ Madrid 17.4.2009 (AS 2009/1656).

L'STC 98/2000, de 10 d'abril (assumpte *Casino La Toja*), va abordar la instal·lació de sistemes audiovisuals de control per a la seguretat del casino i va concloure que calia tenir en compte no només el lloc del centre de treball en què les instal·la l'empresa, sinó també altres elements de judici per dilucidar en cada cas concret si aquests mitjans de vigilància i control respecten el dret a la intimitat dels treballadors. El TC, després d'acudir al test de proporcionalitat, conclou que la mesura d'instal·lació d'un sistema i gravació d'àudio no supera el requisit de necessitat. En aquest sentit, considera que

> «la instalación de los micrófonos no ha sido efectuada como consecuencia de la detección de una quiebra en los sistemas de seguridad y control anteriormente establecidos sino que [...] se tomó dicha decisión para complementar los sistemas de seguridad ya existentes en el casino».

És a dir, no s'acredita que la instal·lació del sistema de captació i gravació de sons sigui indispensable per a la seguretat i el bon funcionament del casino. Així doncs, l'ús d'un sistema que permet l'audició continuada i indiscriminada de tot tipus de converses, tant dels propis treballadors com dels clients del casino, constitueix una actuació que sobrepassa àmpliament les facultats que li atorga a l'empresari l'article 20.3 LET i suposa, en definitiva, una intromissió il·legítima en el dret a la intimitat consagrat a l'article 18.1 CE.

L'STS de 2014.05.13 (u. d. 1685/2013) va declarar il·lícita la gravació d'imatges sense prèvia informació de l'empresa als treballadors o als seus representants legals (per exemple, amb adhesius avisadors sobre l'existència de les càmeres enfocades cap a l'ascensor[63]) en un cas relatiu a possibles incompliments laborals genèrics que es poguessin cometre (entesa com informació prèvia i expressa, precisa, clara i inequívoca de la finalitat de control de l'activitat laboral a què aquesta captació podia ser dirigida), i ha concretat les característiques i l'abast del tractament de dades que es volien realitzar, és a dir, en quins casos els enregistraments podien ser examinats, durant quant de temps i amb

(63)STSJ Galícia 2012.07.06 (Regl. 1464/2012).

quins propòsits, «explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo».

Un supòsit típic de videovigilància lícita el trobem a l'STSJ de Canàries (Tenerife) de 26 d'octubre del 2012 (JUR 2013/23179). El tribunal raona que la mesura d'instal·lació d'una càmera que controlava la zona on el demandant exercia la seva activitat laboral era una mesura justificada (ja que hi havia sospites raonables de la comissió per part de treballadors de greus irregularitats en el seu lloc de treball), idònia per a la finalitat pretesa per l'empresa (verificar si es cometien efectivament les irregularitats sospitades i, en aquest cas, adoptar les mesures disciplinàries corresponents), necessària (ja que la gravació serviria de prova d'aquestes irregularitats) i equilibrada (ja que la gravació d'imatges es va limitar a una determinada zona i durada, la suficient per comprovar que no es tractava d'un fet aïllat o d'una confusió, sinó d'una conducta il·lícita reiterada), per la qual cosa s'ha de descartar que s'hagi produït cap lesió del dret a la intimitat personal consagrat a l'article 18.1 CE.

És veritat que no hi ha normativa específica que reguli la instal·lació i utilització d'aquests mecanismes de control i vigilància consistents en sistemes de captació d'imatges o gravació de sons dins dels centres de treball, de manera que són els òrgans jurisdiccionals els encarregats de ponderar, en cas de conflicte, en quines circumstàncies es pot considerar legítim el seu ús per part de l'empresari, a l'empara del poder de direcció que li reconeix l'article 20.3 ET, i de vigilar que es respectin sempre els drets fonamentals del treballador, i molt especialment el dret a la intimitat personal que protegeix l'article 18.1 de l'esmentada norma fonamental, amb el principi de proporcionalitat sempre present. Per això, el més rellevant en aquest cas és determinar si l'actuació empresarial de vigilància videogràfica amb «càmera oculta» està justificada en unes sospites prèvies que necessiten constatació, de manera que en el marc d'aquesta «constatació» –que s'integra en el dret fonamental a la prova ex article 24 CE– s'ha de verificar si aquesta vigilància supera o no el judici de proporcionalitat subdividit en els tres subjudicis d'idoneïtat, necessitat i proporcionalitat en sentit estricte.

Reforça l'anterior la dada que l'STC 39/2016, de 3 de març, no modifica íntegrament el criteri de l'STC 29/2013, d'11 de febrer, malgrat el que alguns comentaristes d'aquella ho han volgut assenyalar. En efecte, entenc que el que l'STC 39/2016 indica clarament és que, d'acord amb la Instrucció 1/2006, de 8 de novembre, de l'AEPD, «el hecho de que la empresa hubiera colocado un cartel genérico advirtiendo de la existencia de cámaras[64] es suficiente para determinar que los empleados podían conocer la existencia de las cámaras y la finalidad para las que habían sido instaladas». Per tant, no es tracta tant que no se n'informi l'RLT (fet que ja és qüestionable, al meu parer), sinó que ni tan sols s'indiqui amb un simple cartell o panell que seran implantades les càmeres de seguretat.

(64)Que es poden trobar en qualsevol espai públic, botiga, amb l'indicatiu de «zona videovigilada».

No és menys cert que l'STC 29/2013 donava a entendre la necessitat d'una «información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida». Aquesta informació hauria de concretar el següent: «en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo». També és veritat que l'STC 39/2016 allibera les empreses d'aquesta càrrega informativa explícita i precisa, alhora que converteix la sospita que un treballador està cometent irregularitats en una habilitació per instal·lar les càmeres al lloc de treball, una mesura idònia i necessària per a la finalitat buscada, com seria el control de l'activitat laboral dels empleats. En suma, «no olvidemos que la instalación de cámaras de videovigilancia es, en cualquier caso, una medida restrictiva de derechos fundamentales, y como tal se exige superar el triple juicio de proporcionalidad, necesidad e idoneidad». Amb tot, els treballadors es consideraran prou informats amb els cartells estàndards indicatius de «zona videovigilada» si s'aplica «al peu de la lletra» el criteri de l'STC 39/2016.

D'altra banda, l'STS 2017.02.02 (u. d. 554/2016) analitza l'ús de càmeres videogràfiques a la vista dels treballadors quan hi ha sospita d'una conducta irregular, col·locades a l'entrada i als serveis públics d'un gimnàs, exceptuats vestuaris i lavabos, sense que els treballadors hagin estat advertits del seu possible ús amb fins disciplinaris. Un treballador va ser acomiadat, entre altres raons, per obrir amb la seva polsera el torniquet a persones no sòcies perquè accedissin a la instal·lació de manera no autoritzada. Assenyala el TS que, en l'àmbit laboral, el consentiment del treballador per al tractament per part de l'empresa de les seves dades de caràcter personal passa, com a regla general, a un segon pla, «pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de dichos datos sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes y no se lesionen derechos fundamentales del trabajador». Això concorda amb l'article 20.3 de l'ET (el consentiment s'entén implícit en la mateixa acceptació del contracte que implica el reconeixement del poder de direcció de l'empresari).

No obstant això, persisteix el deure d'informació, «debiendo someterse la falta o insuficiencia de esta al juicio de proporcionalidad, lo que requerirá determinar en cada supuesto, con carácter previo, si se ha producido o no la indicada omisión de la información debida ponderando los derechos y bienes constitucionales en conflicto»; és a dir, d'una banda, el dret a la protecció de dades del treballador i, de l'altra, el poder de direcció empresarial. En el cas analitzat, «el trabajador conocía que la empresa había instalado un sistema de control por videovigilancia». Així doncs, aquesta no havia d'especificar, més enllà de la mera vigilància, la finalitat exacta que havia assignat a aquest control. El més important serà determinar si la dada obtinguda s'ha utilitzat per a la finalitat de control de la relació laboral o per a una finalitat aliena al compliment del contracte, perquè només quan la finalitat del tractament de dades no té

relació directa amb el manteniment, desenvolupament o control de la relació contractual, l'empresari estaria obligat a sol·licitar el consentiment dels treballadors afectats. L'ús de la càmera de vídeo va revestir, per tant, «carácter razonable y proporcionado a su objeto», sense que pel lloc de la seva instal·lació hi hagués risc de la vulneració del dret a l'honor, a la intimitat personal i familiar ni per les circumstàncies de temps i oportunitat hi hagués hagut risc per al ple exercici dels seus drets, en haver actuat el treballador com ho va fer: «Siendo conocedor de que su conducta estaba siendo grabada y de que por lo que respecta a las cámaras de la entrada, el acceso indebido con auxilio interno ya había sido objeto de sanción».

L'STS 2017.01.31 (u. d. 3331/2015) analitza el cas d'un dependent que és sorprès manipulant tiquets i furtant diferents quantitats en dates concretes. L'empresa havia informat prèviament de la instal·lació de càmeres per motius de seguretat, però no del destí que es pogués donar a les imatges o la utilització en contra seu. El TS reconeix la procedència de l'acomiadament disciplinari per transgressió de la bona fe contractual i entén com a vàlides les proves de videovigilància emprades per l'empresa, ja que la instal·lació de càmeres era «una medida justificada por razones de seguridad» (control de fets il·lícits imputables a empleats, clients i tercers, així com ràpida detecció de sinistres), idònia per a l'assoliment d'aquest fi (control de cobraments i de la caixa en el cas concret) i necessària i proporcionada al resultat perseguit, raó per la qual estava justificada la limitació dels drets fonamentals en joc, «máxime cuando los trabajadores estaban informados expresamente de la instalación del sistema de vigilancia y de la ubicación de las cámaras por razones de seguridad». Aquesta expressió tan àmplia inclou la vigilància d'actes il·lícits dels empleats i de tercers i, en definitiva, de la seguretat del centre de treball, però exclou un altre tipus de control laboral que sigui aliè a la seguretat, és a dir, el de l'efectivitat en el treball, les absències del lloc de treball, les converses amb companys, etc.

En qualsevol cas, davant els defectes informatius que es puguin al·legar, és procedent reclamar a l'empresa més informació o denunciar-la davant l'Agència Espanyola de Protecció de Dades amb la finalitat d'obtenir una sanció per les infraccions que hauria pogut cometre, però això no disminueix la correcció de l'acomiadament practicat.

La STSJ d'Andalusia-Sevilla de 22 de març del 2017 (rec. 1461/2016) declara com a comiat procedent per «faltas de respeto y de consideración a la dignidad de los pacientes discapacitados» la conducta d'un auxiliar d'una residència geriàtrica que maltractava els residents, una conducta confirmada: «inexistente vulneración del derecho a la intimidad por ser válida la colocación por la empresa de cámaras de videovigilancia en un cuarto de baño utilizado por las auxiliares para bañar a los residentes, ante la sospecha de malos tratos a

estos, teniendo ya cámaras de videovigilancia en el resto de instalaciones con el consentimiento informado de los trabajadores». Així doncs, es tracta d'una mesura raonable i proporcionada.

5. La geolocalització al lloc de treball

En aquest cas parlem de GPS (*global positioning system*) instal·lats en vehicles (rastreig *teletracking* acoblat a una xarxa digital de comunicacions mòbils GSM –*global system for mobile communications*–) o bé de telèfons intel·ligents facilitats per l'empresa. La possibilitat d'instal·lar geolocalitzadors, bé sigui al vehicle (per organitzar amb més eficàcia les rutes, lliuraments, i en general l'ús que s'ha fet del vehicle fora del centre de treball –hores d'arrencada, parades, quilòmetres recorreguts, visites realitzades a clients, quantitat de combustible consumit, etc.–), bé en els dispositius mòbils que es faciliten al treballador, afecta una de les manifestacions del seu dret a la intimitat: el dret «a que los demás no sepan dónde está en cada momento y cuáles son sus movimientos; o dicho en otros términos, el derecho a no estar localizado de manera continua por medios electrónicos colocados en sus bienes contra su voluntad»[65].

(65)STEDH 2 de setembre del 2010, cas *Uzun contra Alemanya*.

Així, les dades de localització per GPS de la ubicació del treballador durant la seva jornada s'han considerat també emparades pel dret a la protecció de dades, i aquestes dades il·lícitament obtingudes, per a una **finalitat diferent** a l'anunciada al treballador per l'empresa, s'han considerat com a **prova il·lícita** a efectes d'acomiadament[66]. En efecte, aquestes sentències importants conclouen, en resum i amb encert, que la possibilitat de conèixer en tot moment, mitjançant un sistema de geolocalització que permet un continu i permanent seguiment del vehicle cedit per a ús professional, no només el posicionament d'aquest per raons de seguretat, sinó també el lloc exacte on es troba el treballador (fins i tot fora de la seva jornada laboral) i, al seu torn, el posterior tractament de les dades obtingudes amb una finalitat completament diferent de l'anunciada i, per tant, sense coneixement del conductor, fan que les conclusions extretes gràcies a aquest dispositiu tecnològic i la seva aportació com a mitjà de prova en seu judicial per demostrar un pretès incompliment contractual constitueixin un procediment que lesiona els drets fonamentals de constant cita. Així ho va considerar la mateixa Agència Espanyola de Protecció de Dades al seu Informe 193/2008, sobre la instal·lació d'un sistema GPS en l'automòbil facilitat a un treballador, en el qual després de reproduir el mandat de l'article 20.3 de l'ET diu amb rotunditat:

(66)SSTSJ Madrid 2014.03.21 (Regl. 1952/2013) i 2014.09.29 (Regl. 1993/2013).

> «No obstante, la existencia de esta legitimación no excluye el cumplimiento del deber de informar, por parte del empresario previsto en el artículo 5.1 de la Ley orgánica. En consecuencia, la actuación descrita en la consulta genera el correspondiente fichero y, en todo caso, será obligatoria su inscripción en el Registro General de Protección de Datos, conforme a lo establecido en el artículo 26 de la Ley orgánica».

Per la seva banda, l'STEDH de 2 de setembre del 2010 (JUR 2010, 301.139), cas *Uzun contra Alemanya*, considera que la instal·lació d'un sistema GPS constitueix una ingerència greu en la vida privada de la persona. No obstant això, no falten a la doctrina judicial pronunciaments contradictoris, que a continuació intentaré sintetitzar:

a) STSJ Castella i Lleó 2013.08.05 (Regl. 453/2013): declara com a **procedent** l'acomiadament d'un treballador que no va concertar visites amb clients durant les tardes d'estiu i que va desviar el telèfon de l'empresa (mòbil amb xarxa de localització), que tenia un sistema de geolocalització, al seu propi, a més d'acudir a la visita d'un client en banyador i xancletes de piscina.

b) STSJ Andalusia-Granada 2015.07.15 (Regl. 1264/2015): declara la procedència de l'acomiadament d'una delegada comercial a partir de les dades GPS generades pel vehicle durant la jornada laboral, que demostren que els informes de visites que es diuen que s'han fet no són certs. En aquest cas no és necessari el «consentiment» previ del treballador per implantar el GPS al cotxe d'empresa. La Sala de suplicació assenyala que

> «los datos GPS utilizados son única y exclusivamente los generados por el movimiento del vehículo utilizado por el trabajador solo en jornada de trabajo y a los exclusivos efectos de realizar las funciones propias de la categoría. Cuestión distinta es que implantado el sistema GPS en un vehículo puesto a disposición del trabajador de manera permanente, por ejemplo, en caso de directivos o comerciales, resultara luego que se intentaran hacer valer los datos obtenidos en relación a tramos horarios ajenos a la jornada laboral y a la prestación de servicios, [...] razón por la cual los datos obtenidos del sistema GPS del vehículo podían utilizarse por la empresa para la comprobación del cumplimiento de los deberes laborales del interesado».

c) STSJ Castella-la Manxa 2015.04.28 (Regl. 134/2015): declara la improcedència de l'acomiadament, perquè la instal·lació de GPS en un vehicle de l'empresa suposa la vulneració del dret a la intimitat personal del treballador (vigilant de seguretat) i entén, contràriament al que sosté l'STSJ Andalusia-Granada 2015.07.15 (Regl. 1264/2015), que el treballador hauria d'haver tingut coneixement previ de la implantació del sistema GPS mencionat[67].

(67)STC 29/2013, d'11 de febrer.

d) STSJ Illes Canàries 2015.11.05 (Regl. 834/2014): la manipulació consci-ent d'un dispositiu de localització del vehicle facilitat al treballador per a l'acompliment de la seva feina (subjecte al xassís del vehicle per mitjà de brides plàstiques amb connector d'antena GPS interior i exterior), de manera que aquest dispositiu quedi inutilitzat, pot suposar acomiadament disciplinari, però sempre que es demostri que aquesta inutilització ha estat obra d'aquell a qui s'imputa, ja que en cas contrari l'acomiadament és, senzillament, improcedent.

És molt coneguda la noció següent que apareix a l'SSTC 114/1984, de 29 de novembre:

«quien graba una conversación de otros atenta, independientemente de toda otra consideración, al derecho reconocido en el artículo 18.3 CE; por el contrario, quien graba una conversación con otro no incurre, por este solo hecho, en conducta contraria al precepto constitucional citado».

El control de l'ús abusiu del telèfon posat a disposició per l'empresa als treballadors és lícit; però, segons l'STSJ Catalunya 26.11.2012 (AS 2013\846),

«la empresa no puede controlar el contenido de las comunicaciones. De esta forma, el control el abuso del teléfono puede realizarse mediante las facturas telefónicas, debiendo la empresa dar instrucciones de uso y no pudiendo controlar el contenido de las llamadas».

L'excepció la constitueix el cas dels treballadors de telemàrqueting: l'STS de 2003.12.05 (RJ 2004, 313), sobre monitorització de trucades de treballadors de telemàrqueting telefònic,

«considera proporcionada dicha "monitorización" o control empresarial, pues el mismo tiene como único objeto controlar la actividad laboral del trabajador en condiciones de respeto a su esfera íntima inatacable (el teléfono controlado se ha puesto a disposición de los trabajadores como herramienta de trabajo para que lleven a cabo sus funciones de telemarketing y a la vez disponen de otro teléfono para sus conversaciones particulares, que no está monitorizado)».

En un altre supòsit, la tolerància d'una empresa pel que fa a l'ús d'un telèfon mòbil genera un cert marge de confidencialitat, de manera que seria improcedent, per exemple, l'acomiadament per utilització de telèfon mòbil i vehicle d'empresa per a fins empresarials en un context de tolerància empresarial[68].

(68)STSJ Madrid 27.6.2007 (Regl. 2233/2007).

També és d'interès és el cas resolt per l'STSJ del País Basc de 2007.07.02 (JUR 2007/365564), a propòsit d'un acomiadament basat en prova de sistema de localització GPS del telèfon mòbil que tenia assignat un treballador (que no sabia la seva existència), ja que entén que conculca la intimitat del treballador, perquè aquest dret

«queda afectado si el empresario utiliza un sistema de control del trabajo de sus empleados que se desarrolla fuera de sus dependencias a través de un sistema de localización permanente del teléfono móvil que se facilita como instrumento de trabajo, sin consentimiento ni conocimiento de aquellos, máxime si estos han de tenerlo a su disposición en todo momento por estar sujetos a disponibilidad permanente, ya que si bien resulta un medio idóneo para controlar su labor (de lo que no le priva que pueda hacerse un uso que le impida realizar esa función, como sucede si el teléfono en cuestión no lo lleva consigo el trabajador), en modo alguno resulta necesario si tenemos en cuenta que el propio sistema de telefonía móvil siempre permite conocer ese dato y, por tanto, acceder a ese conocimiento con autorización judicial si concurren circunstancias que justifican una actuación de esa naturaleza, tan invasora del campo propio de la intimidad personal. Esfera, esta, que ni tan siquiera desaparece durante la jornada laboral, en la que el trabajador mantiene un reducto en el que su empresario no puede penetrar si no resulta preciso por exigencias de la relación laboral, mediante un medio idóneo, necesario y suficientemente proporcionado al sacrificio de ese derecho fundamental».

Finalment, hem de fer esment del cas resolt per la STSJ d'Astúries de 3 d'octubre del 2017 (rec. 1908/2017), en el qual s'acomiada disciplinàriament (comiat qualificat com a procedent per disminució del rendiment i incompliment de l'horari) un comercial que, en lloc de fer les visites que deia, cobrava dietes

(seixanta-vuit en total) quan en realitat menjava a casa, un procediment irregular (cobrament indegut) que va ser detectat mitjançant el GPS instal·lat a la tauleta que l'empresa li havia facilitat.

6. Les relacions sindicals en l'àmbit de les tecnologies de la informació i la comunicació

El tema de l'«ús sindical» dels mitjans TIC a l'empresa (web, correu electrònic) no està exempt de controvèrsies. En efecte, cal recordar que el Tribunal Constitucional ha assenyalat que l'enviament d'aquest tipus de missatges de correu electrònic constitueix un dret dels sindicats emparat pel dret fonamental a la llibertat sindical[69], tot i que s'han de donar «ciertas condiciones, como que la empresa disponga del servicio de correo electrónico» (no és obligatori que el creï només pel fet que els sindicats el reclamin, si no hi ha sistema de comunicació electrònica a l'empresa i el cost és important[70]), que «los envíos de *e-mails* se realicen de modo proporcional» (comunicació i difusió d'informació d'interès laboral o sindical entre els sindicats i els treballadors) i que «con tal envío no se perjudique el normal funcionamiento de la organización empresarial» (l'empresa ha d'acreditar els problemes de funcionament que li suposa la utilització massiva del correu electrònic per part dels sindicats[71]).

[69] STC.281/2005, a manera de *leading case*.

[70] STS 2012.05.17 (rec. 202/2011).

[71] STS 3.5.2011 (rec. 114/2010).

En relació amb el dret d'informació dels sindicats per mitjans electrònics, el parer del TC ha estat compartit per l'STS 2011.06.22 (rec. 153/2010), que afegeix el següent:

> «La introducción en las empresas de medios de comunicación electrónicos en paralelo a los tradicionales o en sustitución de los mismos ha derivado en frecuentes litigios sobre los derechos de los trabajadores en tales nuevos contextos de organización. Las primeras respuestas judiciales a tales conflictos mostraron cierta incertidumbre en cuanto al conocimiento del verdadero alcance de las modificaciones que esa nueva forma de relación produce en el entorno laboral. [...] En síntesis, tales principios se fundamentan en la ponderación del reconocimiento del derecho a la acción sindical en el entorno de comunicación electrónica, pero siempre ponderando los intereses en juego con los que exige la organización empresarial y el coste que el ejercicio de dicho derecho puede tener para la empresa».

La situació actual, lluny de presentar-se mancada d'arestes, segueix generant conflictes. A tall d'exemple, cal citar les resolucions següents:

a) Sentència de l'Audiència Nacional de 2014.05.27 (proced. 83/2014): fins a l'any 2008, tots els sindicats amb presència a la Corporació Ràdio Televisió Espanyola (CRTVE) estaven **autoritzats** a enviar correus electrònics als treballadors de l'empresa, incloent-hi els arxius adjunts que creguessin convenients. A partir del 2008, aquesta política va canviar per evitar que s'adjuntessin documents, amb l'objecte de no saturar l'espai d'emmagatzematge en els equips, després de la introducció d'un sistema d'emmagatzematge al núvol, de manera que el sindicat havia de pujar els documents que volgués distribuir als treballadors a un servidor FTP (*file transfer protocol*) i incloure al cos del correu electrònic enviat als treballadors un enllaç a aquest arxiu perquè el treballador que tingués interès a llegir-lo ho pogués fer. El 2012 es va arribar a un acord amb el comitè intercentres, de manera que cada sindicat va passar a disposar

d'un compte de correu electrònic per a la distribució de comunicacions a tots els treballadors i de cinc més del tipus estàndard, via correu web o Lotus Notes (client de correu a elecció de cada sindicat). El sindicat CGT no té presència al comitè intercentres, però sí als comitès d'empresa de Madrid, Barcelona i Canàries i, fins al març del 2014, podia enviar correus electrònics des del seu compte de correus de CRTVE a tots els treballadors de l'empresa; però, al març del 2014 CRTVE va informar CGT que havia establert un filtre, de manera que des del compte de correu atribuït al sindicat CGT només es podien distribuir correus (enviament massiu) als grups d'usuaris territorials de Madrid, Barcelona i Canàries. Per contra, els altres sindicats podien remetre des dels seus comptes de correu els enviaments massius a tots els grups territorials, és a dir, a tots els treballadors de l'empresa.

L'Audiència Nacional entén que hi ha vulneració del dret a la llibertat sindical de CGT (en el seu vessant de transmetre informació sindical als seus afiliats) perquè l'empresa no va acreditar que els filtres aplicats fossin necessaris per raons de cost o de limitació de la capacitat de la «xarxa» corporativa (fet que va generar una desigualtat de tracte no justificada), de manera que CRTVE no va respectar l'exigència de

> «neutralidad de la red empresarial en los aspectos sindicales, [que ha] de aplicarse sobre los distintos parámetros técnicos de configuración del acceso a la red y el uso de la misma, tanto si se trata de una intranet como del acceso a internet, como pueden ser la creación de cuentas de correo electrónico, la configuración de los buzones de correo, los derechos de acceso al directorio interno de los usuarios, la dotación de espacio en los servidores para alojamiento de archivos, la posibilidad de recibir y/o enviar correo ajeno a la intranet o el establecimiento de filtros de acceso a información o de correo».

Finalment, va fixar una indemnització de 1.500 € per la vulneració de la llibertat sindical de CGT.

b) STS 2016.04.26 (rec. 113/2015): la negativa de l'empresa a publicar a la intranet corporativa comunicats sindicals (de CCOO) basant-se en el seu contingut constitueix una **censura inacceptable**, contrària a la llibertat d'expressió i de transmissió d'informacions sindicals, que confirma la sentència de l'Audiència Nacional del 2014.10.10 (actuacions 207/014), així com la indemnització de 6.000 €.

c) STSJ Andalusia-Sevilla 2015.09.24 (Regl. 1387/2015) analitza la denúncia d'una secció sindical que té limitacions d'accés a internet i correu electrònic, motivades per l'activitat de l'empresa i per la informació confidencial que s'hi mou, i sol·licita que se li concedeixi lliure accés a la totalitat de la xarxa, o si no, a les xarxes socials com Facebook i Twitter, com també al correu propi de la CGT i pàgines similars. La secció sindical disposa d'un ordinador, integrat a la xarxa interna de l'empresa demandada i amb accés a internet en els mateixos termes, condicions i limitacions que li són propis a la resta d'equips informàtics (xarxa informàtica corporativa autoritzada per l'Autoritat Nacional de Seguretat –Centre Nacional d'Intel·ligència del Ministeri de la Presidència– per a la gestió d'informació classificada fins al nivell «difusió limitada», equivalent

a NATO Restricted en l'àmbit de l'OTAN) de què disposa l'empresa demandada (EADS Construcciones Aeronáuticas, SA, que té l'obligació d'implantar i mantenir totes les mesures de seguretat exigides per aquesta autoritat i pel Centre Criptològic Nacional per mantenir la informació classificada que es mou a la seva xarxa). Entén la Sala Social del TSJ Andalusia-Sevilla que aquesta limitació es produeix per la naturalesa de l'empresa (EADS-Casa-Tabalda-Airbus Military) i la informació confidencial que s'hi mou, «lo que le lleva a aplicar estrictos mecanismos de seguridad a los que se ve obligada por los intereses de seguridad nacionales e internacionales en juego y que lleva a conformar una infraestructura autorizada por la Autoridad Nacional de Seguridad» (Centre Nacional d'Intel·ligència del Ministeri de la Presidència), per a la gestió d'informació classificada fins al nivell de «difusió llimitada» equivalent a NATO Restricted en l'àmbit de l'OTAN. En aquest sentit, és

> «absolutamente comprensible que, manejando la empresa información clasificada y hallándose obligada a proteger mediante medidas de seguridad cualquier filtrado o jaqueado de información, el ordenador que pone a disposición de la sección sindical, y que se encuentra en el ámbito de la red interna de la empleadora, deba ser limitado en las mismas condiciones que el resto de los trabajadores. [Es más,] la contrapartida o las excepciones y salvedades a tal principio, constan así mismo en el protocolo de seguridad, y permiten que cualquier trabajador que tenga interés o le sea de utilidad el acceso a una página restringida, acuda a un procedimiento de corrección de bloqueos que puedan resultar excesivos o indebidos, sin que el sindicato actor haya hecho nunca uso de este mecanismo, ni efectuado a la demandada pretensión alguna a este respecto, lo que se revela por primera vez mediante la interposición de la demanda, no constando acreditado –ni siquiera alegado por la sección sindical recurrente– que esta haya puesto en ningún momento en conocimiento de la empresa su deseo o su necesidad de acceder a páginas concretas, a fin de que esta pudiera examinar la posibilidad de habilitarlo».

d) STS 2016.07.14 (rec. 199/2015): lesiona el dret de llibertat sindical de la CGT la negativa d'una empresa a la utilització d'un compte de correu electrònic corporatiu i l'accés a la llista de distribució de correu electrònic a tots els treballadors (massiva, que ja fa servir la direcció de recursos humans i el comitè d'empresa), si no s'al·lega cap tipus de perjudici o gravamen per a l'empresa (Creu Roja espanyola), sinó únicament que no en disposen les altres seccions sindicals «cuando ninguna de ellas lo había solicitado»; fixen la indemnització en 1.500 € per danys i perjudicis. Els motius que avalen el criteri judicial són els següents:

> «No se alega [por la empresa] la concurrencia de problemas organizativos o de gestión que imposibiliten o desaconsejen la utilización por las secciones sindicales de esa misma vía de comunicación electrónica; ni se dice que interfiera en el proceso productivo; ni se invocan posibles sobrecostes económicos de adaptación o modificación del sistema informático, y como hemos visto, tampoco se hace valer como obstáculo la titularidad del nombre del dominio de correo electrónico, que por otra parte ya se ha consentido utilizar al comité de empresa».

e) STS 2016.11.02 (rec. 262/2015): la negativa d'una empresa (Liberbank, SA, Banco de Castilla La Manxa, SA) a publicar a la intranet corporativa circulars i comunicats sindicals (dret d'informació sindical del sindicat de treballadors de crèdit STC-CIC), tot i el compromís previ que havia adquirit de publicar-los sense limitacions (conciliació de conflicte col·lectiu, 2012.11.27: «La empresa se compromete a publicar en la intranet corporativa los comunicados emitidos por las secciones sindicales existentes en el banco, sin ejercer el veto o control

sobre la legalidad de los mismos y/o su veracidad o a si exceden de los límites informativos»), després incomplert, suposa lesió del dret a la llibertat sindical, amb danys i perjudicis quantificats en un import de 6.000 €.

El Tribunal Suprem ha declarat nul·la, en sentència de 24 de juliol del 2017 (rec. 245/2016), la clàusula d'un conveni col·lectiu (d'empresa) que establia que l'empresa havia de saber el contingut dels correus que remetia el sindicat abans d'autoritzar que fossin enviats per mitjà de les llistes de distribució per intranet. El tribunal considera que s'ha produït una vulneració tant del dret a la llibertat sindical (art. 28 CE) com del secret de les comunicacions (art. 18 CE), ja que l'exigència prèvia de control empresarial dels textos i continguts del correu electrònic establerta en el conveni col·lectiu és arbitrària i no disposa de justificació.

Bibliografia

Agència Espanyola de Protecció de Dades. *Guía. La protección de datos en las relaciones laborales* [en línia]. [Data de consulta: desembre del 2017]. <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales2.pdf>.

Guijo Tenreiro, A. (2017, 14 de setembre). «Consecuencias disciplinarias de la "intromisión" de las nuevas tecnologías en la relación laboral» [en línia]. *Orbitados*. [Data de consulta: desembre del 2017]. <http://www.orbitados.com/consecuencias-disciplinarias-de-la-intromision-de-las-nuevas-tecnologias-en-la-relacion-laboral-por-carmen-jover-ramirez/>.

Kippel01 (2017, 15 de novembre). «La justicia del Reino Unido da la razón a Deliveroo y considera autónomos a sus 'riders'» [en línia]. *Kippel01*. [Data de consulta: desembre del 2017]. <https://www.kippel01.com/empresa/la-justicia-de-reino-unido-da-la-razon-a-deliveroo-y-considera-autonomos-a-sus-riders.html>.

Lluch Corell, F. J. (2017, 17 de gener). «El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador» [en línia]. *ElDerecho.com*. [Data de consulta: desembre del 2017]. <http://www.elderecho.com/tribuna/laboral/Comunicaciones-empresa-control-correo-electronico-trabajador_11_1045180003.html>.

Melgar Martinez, L. (2016, 20 de desembre). «Trabajadores, medios tecnológicos y control empresarial» [en línia]. *Diario La Ley* (núm. 2, Secció *Legal Management*). [Data de consulta: desembre del 2017]. <http://diariolaley.laley.es/home/DT0000240074/20161216/Trabajadores-medios-tecnologicos-y-control-empresarial>.

Rojo Torrecilla, E. (2017, 21 de desembre). «El caso Deliveroo Valencia. Importa la realidad (trabajo asalariado), no el nombre (trabajo autónomo). Notas y análisis del Acta de la Inspección de Trabajo y Seguridad Social» [en línia]. Blog personal. [Data de consulta: desembre del 2017]. <http://www.eduardorojotorrecilla.es/2017/12/el-caso-deliveroo-valencia-importa-la.html>.

Todolí, A. (2017, 18 de desembre). «Comentario a la Resolución de la Inspección de Trabajo sobre Deliveroo: son laborales y no autónomos» [en línia]. *Argumentos en Derecho Laboral*. [Data de consulta: desembre del 2017]. <https://adriantodoli.com/2017/12/18/comentario-a-la-resolucion-de-la-inspeccion-de-trabajo-sobre-delivero-son-laborales-y-no-autonomos/>.

Valverde, M.; Navarro, J. E. (2007, 24 d'octubre). «El Supremo impide espiar el e-mail de los empleados» [en línia]. *Expansión.com*. [Data de consulta: desembre del 2017]. <http://www.expansion.com/2007/10/24/juridico/1049656.html>.