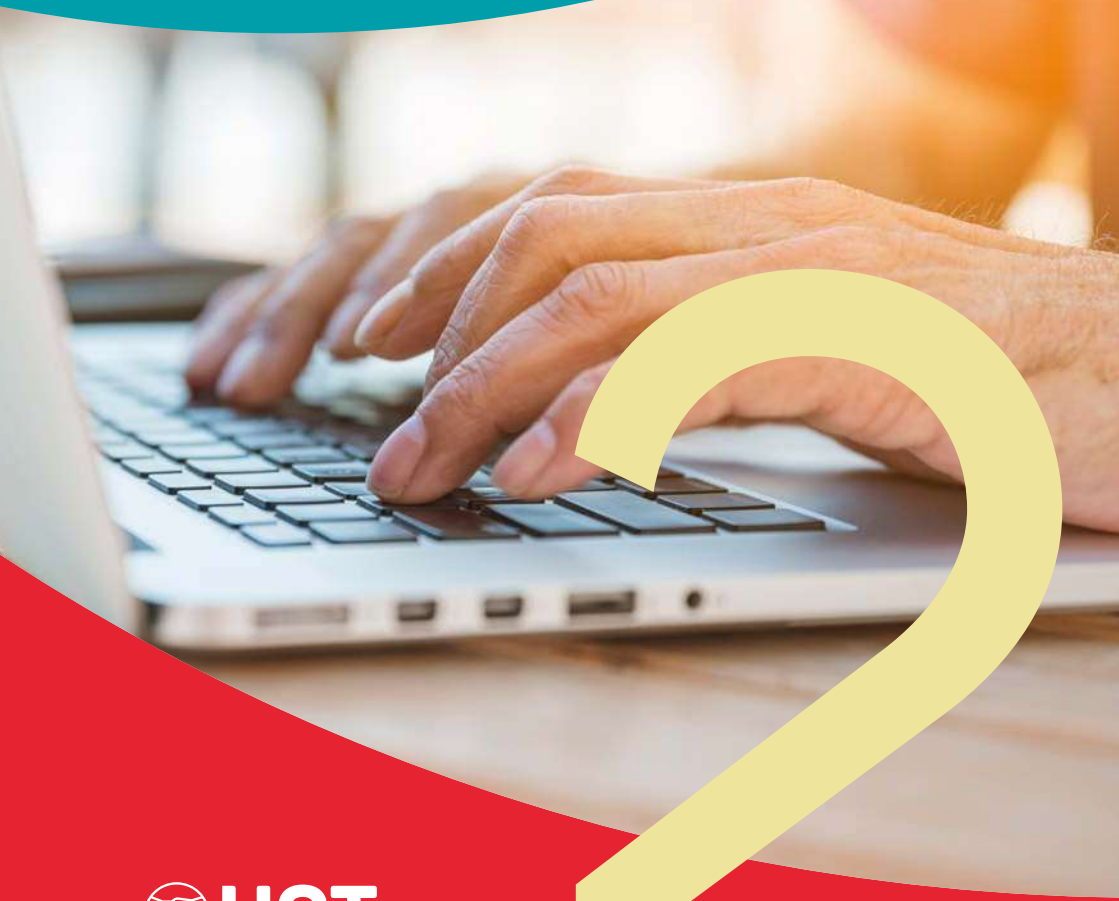
Guia de drets laborals i de prevenció de riscos: IA i vigilància tecnològica

Registre de l'ordinador



2

UGT.cat

Guia de drets laborals i de prevenció de riscos:
IA i vigilància tecnològica

Registre de l'ordinador

Edició:
UGT de Catalunya
2026

Elaboració i redacció:
Dr. Adrián Todolí Signes,
Universitat de València.

Alba Navalón Arnal,
Universitat de València.

Disseny i maquetació:
Manera Estudi

Fotografies:
Magnific

Impressió:
Impremta Pagès

Dipòsit legal:
B 11742-2026

Amb el suport de:

UGT.cat

a la feina cap risc

Generalitat de Catalunya

Guia de drets laborals i de prevenció de riscos: IA i vigilància tecnològica

Registre de l'ordinador

2

Taula de continguts

Presentació

Afrontem un moment de transformació profunda del món del treball. La digitalització, la intel·ligència artificial i els sistemes de control tecnològic no són cap ficció, ja són presents als centres de treball i estan redefinint, de manera accelerada, les relacions laborals, canviant els drets i les condicions laborals de les persones treballadores, així com modificant les relacions de poder. Tal com es recull en aquesta guia, aquesta transformació no és neutra i comporta riscos evidents per a la privacitat, la salut laboral i la dignitat de les persones treballadores.

Davant d'aquest escenari, no podem quedar al marge ni limitar-nos a reaccionar tard. Cal anticipar-nos, comprendre els nous mecanismes de control i actuar amb determinació per garantir que l'avenç tecnològic no es tradueixi en una reculada de drets. Hem de garantir una transició justa davant aquest procés tecnològic i no permetre que cap treballador o treballadora quedi enrere. Som davant d'un nou camp de conflicte laboral: el del control algorítmic, la vigilància digital i l'explotació de dades. En aquest terreny, la negociació col·lectiva, la intervenció sindical i la mobilització són més necessàries que mai, perquè són les eines que permetran afrontar aquesta transició de manera justa i equitativa.

Aquesta guia neix precisament amb aquesta voluntat: dotar la representació sindical i les persones treballadores d'eines per defensar-se en un context cada vegada més complex. No es tracta de rebutjar la tecnologia, sinó de controlar-ne l'ús. La digitalització ha d'estar al servei de les persones, i no a l'inrevés. No acceptarem que es faci servir per intensificar ritmes de treball, per vigilar-nos de manera constant o per justificar decisions automatitzades que escapin a qualsevol control democràtic.

Ara bé, també hem de ser clars i realistes: tal com s'explica al llarg d'aquesta guia, la legislació vigent sovint no protegeix les persones treballadores en el grau que des de la UGT de Catalunya considerem necessari. Hi ha buits, interpretacions flexibles i marges empresarials que permeten pràctiques de control que qüestionem obertament. Precisament per això, és imprescindible conèixer en profunditat aquest marc legal. Només així podrem jugar bé les cartes, utilitzar totes les eines disponibles i guanyar espais en la defensa dels drets laborals.

En aquest sentit, des de la UGT Catalunya reivindiquem que els drets fonamentals, la intimitat, la protecció de dades, la salut laboral i la dignitat han de ser límits infranquejables davant qualsevol innovació tecnològica.

No hi pot haver cap transformació digital justa si no incorpora garanties efectives per a les persones treballadores. La tecnologia no pot convertir-se en una eina de precarització ni de control massiu.

Per a l'elaboració d'aquesta guia hem comptat amb la col·laboració del doctor Adrián Todolí Signes, catedràtic de Dret del Treball i de la Seguretat Social de la Universitat de València, una de les veus més reconegudes en l'anàlisi de l'impacte de la digitalització en les relacions laborals. El seu prestigi acadèmic i el seu compromís amb la defensa dels drets laborals aporten rigor, solidesa jurídica i perspectiva crítica a aquest treball.

Aquesta guia no és només un document informatiu: és una eina de lluita sindical. Davant la implantació de sistemes de videovigilància, geolocalització, biometria o control algorítmic, sovint sense transparència ni negociació, cal reforçar l'organització col·lectiva i exigir drets. Tal com evidencia aquesta anàlisi, moltes d'aquestes pràctiques poden generar riscos psicosocials, incrementar la pressió laboral i aprofundir desigualtats ja existents.

Per això, des de la UGT Catalunya fem una crida: no podem permetre que la revolució digital es construeixi d'esquena a les persones treballadores. Cal situar els drets al centre, reforçar la negociació col·lectiva i garantir la participació sindical en qualsevol implantació tecnològica.

Oscar Riu i Garcia

Secretari Política Sindical de la UGT de Catalunya

Reyes Solaz

Secretària Nacional UGT de Catalunya-Salut Laboral

Introducció

La transformació digital del treball s'ha accelerat de manera intensa en els darrers anys. La incorporació de **tecnologies digitals** als processos productius, a l'organització del treball i als sistemes de gestió de personal ha alterat profundament la relació laboral. Aquest procés no és neutral. Juntament amb oportunitats d'eficiència i innovació, la digitalització està generant **noves formes de control empresarial** que poden afectar de manera directa els drets fonamentals de les persones treballadores.

En aquest nou escenari, la intel·ligència artificial, els sistemes de vigilància digital, el tractament massiu de dades, la geolocalització, els sensors, els algoritmes de gestió o els dispositius intel·ligents s'estan utilitzant cada vegada més per supervisar el rendiment, el comportament i la disponibilitat de la plantilla. Sovint, aquestes pràctiques s'implanten sense una **negociació prèvia real**, amb escassa transparència i amb una clara asimetria de poder entre empresa i persones treballadores. El resultat és un increment del control, una reducció dels espais de privacitat i una pressió creixent sobre el temps, el cos i la conducta de les persones que treballen.

Aquesta guia s'elabora des de la convicció que la tecnologia no pot esdevenir una eina de dominació ni de precarització del treball. La digitalització ha d'estar **al servei de les persones** i no a l'inrevés. Quan s'utilitza per intensificar el ritme laboral, vigilar de manera constant o justificar **decisions disciplinàries automatitzades**, la tecnologia deixa de ser un instrument de progrés i es converteix en una font de **risc laboral, social i democràtic**.

L'objectiu principal d'aquesta guia és posar de manifest els efectes lesius que pot tenir l'ús indiscriminat de tecnologies digitals en l'àmbit laboral, especialment pel que fa a la intel·ligència artificial i als sistemes de control tecnològic. Al mateix temps, la guia vol proporcionar **eines pràctiques i útils** perquè els delegats i delegades sindicals, així com la resta de representants legals de les persones treballadores, puguin defensar de manera efectiva els drets laborals davant aquestes pràctiques.

Aquests sistemes inclouen programes de seguiment de productivitat, videovigilància en temps real, control del correu electrònic, anàlisi de dades generades per dispositius corporatius o sistemes algorítmics d'avaluació. Es tracta de pràctiques que, en molts casos, van molt més enllà del que és estrictament necessari per a l'organització del treball.

Els exemples recents són nombrosos i coneguts. Empreses de logística han implantat dispositius portàtils que rastregen la ubicació i el ritme de treball als magatzems, amb un impacte directe sobre les pauses i la intensificació del treball.

Altres empreses, de repartiment, han utilitzat sistemes de geolocalització per controlar les persones repartidores, generant conflictes recurrents sobre privacitat i temps de treball. En el sector financer, es documenten casos d'ús de programari capaç d'analitzar comunicacions internes per avaluar el rendiment, amb seriosos interrogants sobre transparència i límits del control empresarial.

Aquestes pràctiques no són anecdòtiques. Formen part d'una tendència estructural cap a un model de gestió basat en dades, mètriques i algoritmes. Un model que sovint prioritza la productivitat immediata per damunt del **benestar, la salut i la dignitat** de les persones treballadores. La vigilància tecnològica constant genera nous riscos psicosocials, com l'estrès, l'ansietat, la sensació de control permanent i la por a l'error. Aquests efectes poden derivar en problemes de salut mental, esgotament professional i augment de la sinistralitat laboral.

A més, el control tecnològic no afecta tothom de la mateixa manera. Sovint agreuja desigualtats ja existents. Les dones, especialment en sectors feminitzats i precaritzats, poden veure's sotmeses a una vigilància més intensa, vinculada a estereotips de disponibilitat, rendiment o compromís. Les persones amb contractes temporals, jornades parcials o situacions de major vulnerabilitat laboral tenen menys capacitat per qüestionar o resistir aquests sistemes. La tecnologia, lluny de corregir desigualtats, pot acabar reforçant-les.

Un altre risc especialment greu és la utilització de les dades recollides per justificar **sancions, penalitzacions o acomiadaments**. Quan la informació generada per sensors, aplicacions o algoritmes s'utilitza sense garanties, sense possibilitat de contradicció i sense intervenció humana real, es debilita la seguretat jurídica i l'estabilitat en l'ocupació. Això situa les persones treballadores en una posició de vulnerabilitat permanent.

Davant aquest escenari, l'**acció sindical** és imprescindible. La defensa dels drets laborals en l'era digital no pot quedar limitada a l'aplicació mínima de la normativa existent. Cal una intervenció activa, informada i estratègica per part dels sindicats, especialment en l'àmbit de la **negociació col·lectiva**. Els convenis col·lectius són una eina fonamental per establir límits clars al control tecnològic, introduir garanties addicionals i assegurar que la tecnologia s'utilitza de manera proporcional, transparent i respectuosa amb els drets fonamentals.

Aquesta guia neix amb aquesta vocació. Està pensada com un instrument pràctic per als delegats i delegades d'UGT Catalunya, així com per a les persones afiliades, amb l'objectiu de facilitar el coneixement dels drets individuals i col·lectius davant el control tecnològic. La guia ofereix exemples concrets dels usos més habituals de la tecnologia per part de les empreses i analitza, de manera clara i entenedora, quins són els límits legals i sindicals en cada cas.

Al llarg del document s'aborden qüestions clau com la videovigilància, la geolocalització, els sistemes biomètrics, el control de l'ordinador i del telèfon mòbil, el registre de jornada, el control algorítmic, l'ús de sensors, rellotges intel·ligents o equips de protecció individual amb intel·ligència artificial integrada. Cada apartat incorpora preguntes i respostes pensades per resoldre situacions conflictives reals que es troben habitualment els representants sindicals en els centres de treball.

Finalment, la guia posa un èmfasi especial en els **drets col·lectius**. La transparència, el dret d'informació, el dret de consulta i la participació sindical són elements centrals per equilibrar el poder davant la digitalització. Sense aquests drets col·lectius, la tecnologia es desplega de manera unilateral i opaca. Amb ells, és possible condicionar-ne l'ús i orientar-lo cap a models més justos.

En definitiva, aquesta guia vol contribuir a reforçar la capacitat d'UGT Catalunya per liderar una resposta sindical sòlida davant el control tecnològic. Una resposta que no rebutgi la tecnologia, però que tampoc l'accepti acríticament. Una resposta que situï els drets, la salut i la dignitat de les persones treballadores al centre de la transformació digital del treball.

Drets individuals en matèria de privacitat i prevenció de riscos laborals

Davant el registre de l'ordinador i del telèfon mòbil

El terme "dispositius digitals" es limita a l'ordinador o també abasta els telèfons mòbils, les aplicacions, els correus electrònics corporatius, etc.?

La Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD), a l'article 87, introdueix unes especificacions relatives a l'ús de dispositius digitals en l'àmbit laboral i el possible registre del seu contingut per part de l'empresa. Les previsions recollides en aquest precepte afecten la utilització de qualsevol instrument electrònic posat a disposició per l'empresa, ja sigui ordinadors, telèfons mòbils, tauletes tàctils, etc. o aplicacions que es trobin descarregades en aquests, p. ex., sistemes de missatgeria instantanis, correus electrònics corporatius, navegadors web, etc. En definitiva, queden englobats aquells mitjans digitals que emmagatzemen dades que poden arribar a ser privades, ja que, un accés als mateixos pot afectar el dret a la intimitat de les persones treballadores.

Pot l'empresa accedir al contingut dels dispositius digitals propietat de les persones treballadores?

L'ús de dispositius personals per part de les persones treballadores no es troba expressament regulat en la normativa vigent. No obstant això, encara que

l'article 87 de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals no ho esmenti de forma específica, l'empresa ha de, en tot cas, garantir el dret a la intimitat de les persones treballadores quan utilitzin els seus propis dispositius per a fins laborals.

En determinades circumstàncies, les persones treballadores poden emprar els seus dispositius personals per a l'acompliment de la seva activitat professional. L'accés empresarial a aquests dispositius podria suposar una ingerència especialment greu en el dret a la intimitat i/o en el dret a la protecció de dades, atès que s'hi emmagatzema i gestiona informació privada i personal.

De fet, l'Audiència Nacional, en la seva Sentència núm. 13/2019, de 6 de febrer de 2019 (que va ser posteriorment confirmada per la Sentència del Tribunal Suprem núm. 163/2021, de 8 de febrer de 2021) va declarar la nul·litat d'una mesura empresarial que obligava les persones treballadores amb categoria de repartidor/a a aportar un telèfon mòbil de la seva propietat, i a instal·lar-hi una aplicació informàtica de l'empresa que permetia conèixer la geolocalització de la persona treballadora per entendre que no era proporcionada. Es va considerar que aquesta mesura era contrària al dret a la protecció de dades de les persones treballadores per no superar el principi de proporcionalitat, ja que hauria estat possible implantar un sistema de geolocalització en un dispositiu propietat de l'empresa que no impliqués l'accés a dades personals. En el supòsit analitzat, per poder descarregar l'aplicació utilitzada calia facilitar informació com el número de telèfon o l'adreça de correu electrònic, la qual cosa suposava un tractament injustificat de dades de caràcter personal.

En conseqüència, amb caràcter general, no resulta justificat que l'empresa accedeixi al contingut dels dispositius personals de les persones treballadores, entenent-se que, en aquests supòsits, es requeriria el consentiment exprés i lliure de la persona treballadora.

Pot l'empresa registrar els dispositius digitals de les persones treballadores quan han estat atorgats per la mateixa empresa?

Els dispositius que són posats a disposició per l'empresa a les persones treballadores no són considerats efectes particulars, de manera que el seu registre no està subjecte a les garanties previstes en l'article 18 de l'Estatut dels Treballadors (assistència d'un/a representant legal o d'una altra persona treballadora, etc.). En tractar-se de dispositius de propietat empresarial, l'empresa podrà realitzar un examen del seu contingut en virtut de les seves potestats de control i direcció (art. 20.3 ET). De fet, la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals preveu expressament la possibilitat que l'empresa pugui accedir al contingut

dels dispositius digitals facilitats a les persones treballadores (art. 87 LOPDGDD).

No obstant això, la possibilitat de registrar els dispositius digitals no eximeix l'empresa del compliment d'unes garanties. L'empresa, en l'accés als continguts dels dispositius, haurà de respectar el dret a la intimitat de les persones treballadores, observar el principi de proporcionalitat i complir amb la resta de les exigències establertes en la normativa.

Quines garanties estableix la LOPDGDD per a l'accés al contingut d'un dispositiu digital?

D'acord amb la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD), per poder accedir al contingut dels dispositius digitals atorgats a les persones treballadores, l'empresa haurà de complir amb les següents premisses:

- Només podrà accedir als continguts dels dispositius digitals per controlar el compliment de les obligacions laborals o estatutàries o per garantir la integritat dels dispositius (art. 87.2 LOPDGDD).
- Haurà d'elaborar uns criteris d'utilització dels dispositius digitals amb la participació de la RLPT. Aquests criteris hauran, en tot cas, de respectar els estàndards mínims de protecció de la intimitat de les persones treballadores d'acord amb els usos socials i els drets reconeguts constitucionalment i legalment (art. 87.3 LOPDGDD).

Es tracta d'un deure que té caràcter imperatiu, és a dir, l'empresa té l'obligació d'elaborar els criteris d'ús quan proporcioni a les persones treballadores dispositius digitals per a la realització del treball.

- Haurà d'informar les persones treballadores dels criteris d'utilització elaborats i de la possibilitat de realitzar controls sobre l'ús o contingut del dispositiu digital (art. 87.3 LOPDGDD).

Quin ha de ser el contingut dels criteris d'utilització?

La normativa no estableix concretament quina informació ha d'incloure els criteris d'utilització. No obstant això, aplicant la jurisprudència (Sentència del Tribunal Suprem de 26 de setembre de 2007, rec. 966/2006 i Sentència del Tribunal Europeu de Drets Humans, de 5 de setembre de 2017, Cas Bărbulescu contra Romania), es pot concloure que l'empresa haurà d'indicar en els criteris d'ús dels dispositius digitals:

- Les prohibicions d'ús, absolutes o parcials; és a dir amb quines finalitats pot utilitzar la persona treballadora el dispositiu.

Si es permet l'ús amb finalitats privades, l'empresa haurà d'especificar de manera precisa els usos autoritzats i s'hauran d'establir garanties per preservar la intimitat de les persones treballadores. La normativa posa com a exemple de garantia la determinació dels períodes en què els dispositius podran ser emprats amb finalitats particulars (art. 87.3 LOPDGDD).

- La possibilitat que l'empresa realitzi un registre dels dispositius amb fins de control i les conseqüències disciplinàries que en poguessin derivar.
- Les eines de control que seran emprades per vigilar el compliment de les obligacions laborals.

S'ha d'informar les persones treballadores del contingut dels criteris d'utilització?

Les persones treballadores hauran de ser informades dels criteris d'utilització que siguin elaborats per l'empresa (art. 87.3 LOPDGDD). Aquesta informació haurà de ser transmesa amb caràcter previ a l'ús dels dispositius digitals, ja que la persona treballadora ha de ser informada amb antelació de l'abast i la naturalesa de les activitats de monitoratge i de la possibilitat que l'empresa accedeixi al contingut dels dispositius (Sentència del Tribunal Europea de Drets Humans, de 5 de setembre de 2017, Cas Bărbulescu contra Romania).

Per això, no serà vàlida la informació simultània a la intervenció o registre (Sentència del Tribunal Superior de Justícia de la Regió de Múrcia, núm. 82/2022, de 26 de gener de 2022).

Si el conveni col·lectiu tipifica com a falta l'ús de dispositius informàtics propietat de l'empresa amb finalitats no professionals, s'entén que han estat complerts els deures d'informació?

L'empresa ha d'informar sobre els criteris d'ús dels dispositius digitals a les persones treballadores (art. 87.3 LOPDGDD). En principi, aquest deure d'informació no es pot entendre complert quan el conveni col·lectiu tipifica com a falta la utilització de dispositius propietat de l'empresa amb finalitats no professionals. És a dir, encara que de l'establert en el conveni es dedueixi que la persona treballadora no pot utilitzar el dispositiu amb finalitats particulars, aquest criteri d'ús haurà de ser informat expressament a les persones treballadores.

S'entén complert el deure d'informació si les persones treballadores coneixien que una altra persona treballadora havia estat sancionada per emprar els dispositius amb finalitats personals?

La Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals estableix que les persones treballadores hauran de ser informades dels criteris d'utilització dels dispositius digitals elaborats per l'empresa (art. 87.3 LOPDGDD). Per això, si l'empresa decideix prohibir l'ús dels dispositius amb finalitats particulars i establir mesures disciplinàries per a qui incompleixi la prohibició, haurà de transmetre aquesta informació a les persones treballadores. En conseqüència, el fet que les persones treballadores coneguin que una persona treballadora hagi estat sancionada per emprar els dispositius amb finalitats alienes a l'àmbit laboral no serà suficient, en principi, per entendre complert el deure d'informació.

És vàlida la prova obtinguda quan no han estat elaborats els criteris d'utilització?

Quan l'empresa proporciona a les persones treballadores dispositius digitals per a la realització de la prestació laboral, l'empresa té l'obligació d'elaborar uns criteris d'utilització d'aquests dispositius (art. 87.2 LOPDGDD). Per això, si accedeix al contingut d'un dispositiu d'una persona treballadora, per corroborar, per exemple, la comissió d'un acte il·lícit, sense haver prèviament complert amb aquesta obligació s'ha d'entendre, en principi, que la prova obtinguda no seria vàlida; en haver-se produït una lesió del dret fonamental a la intimitat. La

lesió es produeix perquè la persona treballadora no té coneixement que l'empresa pot accedir al contingut dels dispositius digitals. Si no s'estableix expressament que els dispositius no poden ser emprats amb finalitats privades, la persona treballadora pot entendre que té certa privacitat en l'ús de les eines digitals de treball (p. ex., Sentència del Tribunal Superior de Justícia de Canàries núm. 347/2023, de 21 d'abril de 2023).

Aquest criteri ja era sostingut per la jurisprudència abans de l'aprovació de l'article 87.3 LOPDGDD (p. ex., Sentència del Tribunal Suprem, de 8 de març de 2011, rec. 1826/2010).

I si no han estat informades les persones treballadores, és vàlida la prova?

L'empresa ha d'informar amb caràcter previ a les persones treballadores sobre els criteris d'utilització dels dispositius digitals que ha elaborat (art. 87.3 LOPDGDD). En el cas que es registri un mitjà tecnològic sense haver complert amb els deures d'informació es podria considerar que hi ha hagut una vulneració del dret a la intimitat de la persona treballadora. Això es produeix principalment perquè la persona treballadora ha de conèixer si pot emprar el dispositiu amb finalitats privades o si, per contra, la seva utilització ha de quedar limitada a usos professionals. En absència d'aquesta informació, la persona treballadora pot entendre que té certa expectativa de privacitat, és a dir, pot arribar a la conclusió que l'empresa no controlarà el contingut dels dispositius i que els pot fer servir, per tant, per a fins personals.

Per això, si l'empresa realitza un registre sense haver informat dels criteris d'ús, la prova obtinguda, en principi, seria il·lícita, en haver mediat una vulneració de drets fonamentals en la seva obtenció (p. ex., Sentència del Tribunal Superior de Justícia de la Regió de Múrcia núm. 82/2022, de 26 de gener de 2022).

Poden els tribunals considerar que els criteris d'utilització vulneren el dret a la intimitat de les persones treballadores?

Els criteris d'utilització podrien ser declarats nuls si els tribunals entenen que vulneren un dret fonamental (art. 182.1.b) LRJS), com el dret a la intimitat.

Aquest supòsit podria produir-se, per exemple, quan la política empresarial atorgui a l'empresa la facultat d'accedir de forma indiscriminada, continuada i absoluta als dispositius digitals. De fet, el Tribunal Suprem en la Sentència núm. 225/2024, de 6 de febrer de 2024, tot i no analitzar el contingut dels criteris d'utilització que havia confeccionat l'empresa, assenyala que "tan

àmplies possibilitats d'accés poguessin, en el seu cas, col·lidir greument amb els drets a la intimitat i dignitat dels treballadors", qualificant de discutible el contingut dels criteris. La política empresarial sobre l'ús dels dispositius digitals, en aquest cas, establia que: "[...] tots els ordinadors i totes les adreces de correu electrònic corporatius facilitats per l'EMPRESA al TREBALLADOR o utilitzats per aquest en ocasió del seu treball, seran accessibles per l'EMPRESA, podent ser els ordinadors, el seu contingut així com qualsevol arxiu guardat en els mateixos pel TREBALLADOR en qualsevol moment, analitzats, examinats, formatjats i/o restablerts mitjançant els oportuns mitjans informàtics a l'abast de l'empresa (auditoria informàtica, examen pericial informàtic, programari de captura de pantalles, etc.)".

Establerts els criteris d'utilització, quan pot l'empresa registrar els dispositius digitals?

Les persones treballadores tenen dret a la protecció de la seva intimitat en l'ús dels dispositius digitals proporcionats per l'empresa (art. 87.1 LOPDGDD). Per tant, qualsevol accés o registre que es realitzi sobre els dispositius haurà de respectar el dret a la intimitat de les persones treballadores.

Per valorar si la mesura de control establerta per l'empresa vulnera o no el dret a la intimitat de les persones treballadores, s'haurà d'acudir, en primer lloc, a l'establert en els criteris d'utilització dels dispositius digitals (sense perjudici que el seu contingut pugui ser revisat pels tribunals).

- Quan la política empresarial permet l'ús particular dels dispositius, s'aplica un nivell de protecció de la intimitat de la persona treballadora més reforçat o estricte, principalment perquè s'entén que la persona treballadora emmagatzemarà informació privada i personal en el dispositiu. Per aquesta raó, la normativa estableix que l'empresa haurà d'especificar els usos autoritzats i establir garanties per preservar la intimitat de les persones treballadores (art. 87.3 LOPDGDD).

En aquests supòsits, les facultats de control de l'empresa es veuen limitades i només en situacions excepcionals i justificades podria accedir al contingut (p. ex., si s'ha establert expressament que una aplicació no podrà ser utilitzada amb finalitats particulars).

- Quan la política empresarial prohibeix l'ús personal dels dispositius, el nivell de protecció de la intimitat de la persona treballadora disminueix. No obstant això, fins i tot en aquests supòsits, s'entén que la intimitat de les persones treballadores no desapareix. Per això, no quedarà justificada qualsevol mesura de control, sinó aquelles que responguin a una raó legítima i compleixin amb el principi de proporcionalitat.

De fet, la normativa reconeix que s'haurà de respectar, en tot cas, els estàndards mínims de protecció de la intimitat d'acord amb els usos socials i els drets reconeguts constitucionalment i legalment (art. 87.3 LOPDGDD).

Si es prohibeix l'ús privat dels dispositius digitals, s'entén que l'empresa pot accedir al seu contingut en qualsevol cas?

L'empresa ha d'elaborar, amb la participació de la RLPT, els criteris d'utilització dels dispositius digitals i ha d'informar posteriorment sobre el seu contingut les persones treballadores. Dins dels criteris d'ús, l'empresa pot decidir prohibir que els dispositius digitals siguin emprats amb finalitats particulars. No obstant això, encara que l'empresa compleixi amb les exigències legals (participació de la RLPT i informació a les persones treballadores) i limiti l'ús de les eines electròniques facilitades a l'àmbit estrictament professional, per poder accedir al seu contingut (sense vulnerar el dret a la intimitat de les persones treballadores) haurà de complir addicionalment amb els següents requisits:

- *Raó legítima*. L'empresa ha de justificar que el registre o el monitoratge del contingut dels dispositius digitals respon a una raó legítima.

Entre les finalitats considerades legítimes pels tribunals s'inclou la comprovació de sospites sobre la possible comissió d'una irregularitat per part d'una persona treballadora. Així ho il·lustra el supòsit recollit en la Sentència del Tribunal Suprem núm. 119/2018, de 8 de febrer de 2018, que descriu un cas en el qual l'empresa va accedir al correu electrònic d'una persona treballadora per corroborar si havia rebut transferències i regals d'un proveïdor de l'empresa. Les sospites van sorgir perquè una altra persona treballadora va trobar a la fotocopiadora general del lloc de treball dos resguards de transferències bancàries dirigides al seu nom. Es va considerar que el registre estava justificat i la prova era lícita.

No obstant això, és rellevant tenir en consideració que les sospites han de ser significatives. La Sentència del Tribunal Superior de Justícia de Catalunya núm. 2418/2022, de 20 d'abril de 2022 va entendre, per exemple, que l'accés a l'ordinador de la persona treballadora acomiadada havia estat injustificat, ja que l'únic motiu del seu registre va ser la visualització d'emoticones en una aplicació de missatgeria no autoritzada a l'ordinador d'una altra persona treballadora diferent. Una motivació que l'empresa va relacionar amb les sospites que havien estat abocades sobre la persona treballadora acomiadada d'una possible conducta d'assetjament cap a altres membres de la plantilla. El Tribunal va considerar que el registre no estava justificat perquè no havia estat provada la vinculació entre les emoticones i la persona acomiadada ni la possible imputació d'assetjament laboral.

- *Principi de proporcionalitat*. La mesura de control haurà de superar a més el principi de proporcionalitat:
  - Ha de ser idònia, és a dir, susceptible d'aconseguir l'objectiu proposat.
  - Ha de ser necessària, és a dir, que no existeixi una altra mesura més moderada per a la consecució d'aquest objectiu i igual d'eficaç.
  - Ha de ser proporcionada en sentit estricte, és a dir, que aporti més beneficis per a l'interès general que perjudicis sobre altres béns o valors en conflicte.

En termes generals, el principi de proporcionalitat exigeix demostrar que la finalitat no podia ser assolida amb altres mètodes menys intrusius i que el registre es va limitar a l'estrictament necessari i no es va realitzar de forma indiscriminada.

Un supòsit en el qual es va considerar proporcionat l'accés al compte de correu electrònic corporatiu de la persona treballadora és el descrit en la Sentència del Tribunal Suprem núm. 119/2018, de 8 de febrer de 2018. La recerca es va limitar a l'objectiu de trobar correus relacionats amb les transferències bancàries trobades a la fotocopiadora; emprant-se paraules claus i acotant el registre a les dates pròximes a les transferències.

No obstant això, en altres supòsits no s'ha entès superat el principi de proporcionalitat, per exemple, quan:

- Es va gravar la pantalla de l'ordinador de la persona treballadora durant tres dies per comprovar si treballava durant la seva jornada. Es va considerar que aquest monitoratge era excessiu perquè permetia fins i tot visualitzar correus personals i a més ja hi havia testimonis (altres persones treballadores) que podien demostrar que la persona no estava treballant la major part del temps (Sentència del Tribunal Superior de Justícia de Madrid núm. 591/2018, de 13 de setembre de 2018).

Encara que l'empresa prohibeixi l'ús privat dels dispositius digitals, només pot accedir-ne al contingut si hi ha una justificació legítima i el control és necessari, limitat i proporcional.

- Es va instal·lar un programa informàtic en tots els ordinadors propietat de l'empresa per monitorar el seu ús i comprovar si les persones treballadores empraven l'ordinador amb finalitats particulars. Es va acomiadar una persona treballadora perquè accedia a pàgines web alienes a l'àmbit professional. Es va entendre que no era proporcionada la mesura perquè l'objectiu podia aconseguir-se amb mètodes menys intrusius com la restricció de l'accés a certes pàgines web o la supervisió del trànsit en internet o de l'ús de la missatgeria electrònica, però sense examinar el seu contingut (Sentència del Tribunal Superior de Justícia de la Comunitat Valenciana núm. 3390/2018, de 19 de novembre de 2018).

Quan es tracta de l'accés al contingut dels correus electrònics, s'apliquen els mateixos criteris?

L'ús del correu electrònic corporatiu també ha de quedar regulat en els criteris d'utilització, que han de ser elaborats amb la participació de la RLPT i comunicats posteriorment a les persones treballadores. L'empresa podrà accedir als correus electrònics quan s'hagi previst en els criteris d'utilització, existeixi una finalitat legítima i la intervenció respecti el principi de proporcionalitat (és a dir, superi els principis d'idoneïtat, necessitat i proporcionalitat en sentit estricte).

La peculiaritat del compte de correu corporatiu és que la persona treballadora hi pot accedir des del seu dispositiu personal, és a dir, no cal que l'empresa li proporcioni un ordinador o un telèfon mòbil per al seu ús. En aquests supòsits, l'empresa no podrà registrar el dispositiu digital propietat de la persona treballadora, sinó que haurà d'accedir al compte a través del seu servidor.

Pot l'empresa redirigir els correus de les persones treballadores?

Per poder redirigir el compte de correu electrònic d'una persona treballadora en moments, per exemple, en els quals la persona es troba en un període d'incapacitat temporal, l'empresa haurà d'haver informat prèviament les persones treballadores de l'existència d'aquesta possibilitat. No obstant això, la regla general és que, sense una justificació, no és possible redirigir el correu electrònic de forma permanent perquè de fer-ho s'entén que es vulnera el dret a la intimitat de la persona treballadora afectada (Sentència del Tribunal Superior de Justícia de Canàries núm. 17/2023, de 17 de gener de 2023).

A més, no s'hauria de permetre l'accés als correus que es troben a la bústia, sinó simplement la redirecció dels nous correus que siguin rebuts.

Pot el cap o altres companys tenir accés a les claus del correu corporatiu d'una persona treballadora?

Per poder tenir accés al compte de correu corporatiu d'una persona treballadora, l'empresa haurà d'haver informat prèviament les persones treballadores de l'existència d'aquesta possibilitat. No obstant això, la regla general és que, sense una justificació, no és possible compartir les claus de forma permanent perquè de fer-ho s'entén que es vulnera el dret a la intimitat de la persona treballadora afectada.

Es pot accedir al correu electrònic o al dispositiu digital proporcionat després que s'hagi extingit la relació laboral?

Amb caràcter general, l'accés al correu electrònic corporatiu o al dispositiu digital de la persona treballadora després de l'extinció de la relació laboral s'ha considerat que no vulnerava el dret a la intimitat quan l'empresa havia prohibit expressament el seu ús per a finalitats personals i havia ofert a la persona treballadora la possibilitat d'eliminar la seva informació privada abans de procedir a l'accés.

Aquesta és l'argumentació que han seguit diferents tribunals per admetre l'accés al correu electrònic corporatiu o al dispositiu mòbil proporcionat per l'empresa un cop extingida la relació laboral (Sentència del Tribunal Superior de Justícia d'Astúries núm. 1292/2023, de 24 d'octubre de 2023; Sentència del Tribunal Superior de Justícia de Madrid núm. 556/2021, de 30 de juny de 2021).

Per contra, quan la política interna permetia l'ús personal ocasional dels mitjans informàtics i es va accedir als correus electrònics sense autorització judicial, s'ha considerat que hi havia hagut vulneració dels drets a la intimitat i al secret de les comunicacions (Sentència del Tribunal Superior de Justícia de Madrid núm. 328/2022, de 30 de març de 2022).

En qualsevol cas, resulta recomanable que els criteris d'ús dels mitjans digitals de l'empresa prevegin expressament què succeeix després de l'extinció de la relació laboral, incloent-hi el bloqueig dels comptes i la possibilitat que la persona treballadora elimini la seva informació personal, especialment quan s'hagi permès l'ús amb finalitats particulars. Aquestes previsions contribueixen a garantir la intimitat de les persones treballadores i a prevenir conflictes derivats de l'accés a dades personals després del cessament de la relació laboral.

Quines conseqüències pot tenir un incompliment de la normativa aplicable en l'ús de dispositius digitals?

Un incompliment de la normativa que regula l'ús de dispositius digitals en el lloc de treball –p. ex., no haver informat les persones treballadores dels criteris d'utilització– pot suposar una vulneració de drets fonamentals, principalment del dret a la intimitat (art. 18.1 CE). Per això, les persones treballadores, davant d'una potencial lesió dels seus drets fonamentals a causa de la inobservança de la normativa per part de l'empresa, podran presentar demanda de tutela de drets fonamentals expressant els fets que han constituït la vulneració, el dret infringit i la quantia de la indemnització pretesa (arts. 177 i ss LRJS). Igualment, quan la mesura afecti un grup genèric de persones treballadores o un col·lectiu genèric susceptible de determinació individual, els sindicats que tinguin un àmbit d'actuació igual o major al del conflicte també podran iniciar un procediment judicial.

Si queda provada la vulneració de drets fonamentals, la sentència, d'acord amb les pretensions exercitades, podrà declarar la nul·litat radical de l'actuació empresarial, ordenar el cessament immediat de l'actuació que lesiona drets fonamentals i disposar la reparació del dany causat, entre d'altres (art. 182 LRJS). Dins de la reparació de les conseqüències que sorgeixen de la lesió de drets fonamentals, es troba l'abonament d'una indemnització, la quantia de la qual ha estat determinada, en procediments relacionats amb l'ús de dispositius digitals i l'accés al seu contingut, en:

- 600 euros (a cada persona treballadora), per vulneració del dret a la intimitat, en haver redirigit els comptes de correu electrònics de dues persones treballadores en situació d'incapacitat temporal sense comunicació prèvia ni consentiment (Sentència del Tribunal Superior de Justícia de Canàries núm. 17/2023, de 17 de gener de 2023).
- 35.000 euros, per vulneració del dret a la intimitat i del dret al secret de les comunicacions en haver accedit als correus electrònics una vegada extingida la relació laboral sense autorització judicial (Sentència del Tribunal Superior de Justícia de Madrid núm. 328/2022, de 30 de març de 2022).

L'incompliment de la normativa sobre dispositius digitals pot vulnerar drets fonamentals com la intimitat i donar lloc a demandes judicials, nul·litat de les actuacions empresarials i indemnitzacions per danys.

La vulneració de drets fonamentals també pot tenir lloc en l'obtenció de la prova que és emprada per l'empresa per acreditar un acomiadament d'una persona treballadora. En aquests supòsits, la persona treballadora podrà presentar demanda per acomiadament, al·legant que la prova ha de ser declarada il·lícita en haver mediat vulneració de drets fonamentals (art. 90.2 LRJS). Si no s'admet la prova i l'empresa no pot provar la infracció comesa per la persona treballadora per altres mitjans, l'acomiadament serà declarat improcedent (entre d'altres, Sentència del Tribunal Superior de Justícia de la Regió de Múrcia núm. 82/2022, de 26 de gener de 2022; Sentència del Tribunal Superior de Justícia de Catalunya núm. 2418/2022, de 20 d'abril de 2022) o nul (entre d'altres, Sentència del Tribunal Superior de Justícia d'Aragó núm. 454/2022, de 13 de juny de 2022; Sentència del Tribunal Superior de Justícia de Catalunya núm. 3549/2021, de 5 de juliol de 2021); depenent de si l'òrgan judicial entén que la lesió de drets fonamentals es projecta també sobre la decisió extintiva. A més, la declaració de nul·litat o improcedència de l'acomiadament podria anar acompanyada del reconeixement d'una indemnització per danys morals.

Pot ser sancionada l'empresa per un incompliment de la normativa laboral?

Si l'empresa infringeix els preceptes de la normativa laboral relatius a l'ús dels dispositius digitals en el lloc de treball, les persones treballadores i/o la representació legal poden denunciar aquesta situació davant l'autoritat competent, en aquest cas la Inspecció de Treball i Seguretat Social.

Entre les infraccions que podrien ser sancionades per la ITSS en matèria d'ús de dispositius digitals es troben:

- Els actes de l'empresa que siguin contraris al respecte a la intimitat i consideració deguda a la dignitat de les persones treballadores (art. 8.11 LISOS). Es tracta d'una infracció molt greu que pot ser sancionada amb multa, en el seu grau mínim, de 7.501 a 30.000 euros; en el seu grau mitjà de 30.001 a 120.005 euros; i en el seu grau màxim de 120.006 euros a 225.018 euros.

Finalment, cal esmentar que l'Agència Espanyola de Protecció de Dades no té competència per garantir el compliment ni l'exercici de les garanties establertes a l'article 87 LOPDGDD, tal com es recull a la Resolució E/10250/2019, de 3 de juny de 2020[1].

1 Vegeu: https://www.aepd.es/documento/e-10250-2019.pdf

Drets col·lectius davant el control tecnològic

Té dret la RLPT a participar en l'elaboració dels criteris d'utilització dels dispositius digitals atorgats per l'empresa a les persones treballadores?

Quan una empresa lliura dispositius digitals a les persones treballadores per al desenvolupament de la seva activitat laboral, ha d'elaborar els criteris d'utilització d'aquests dispositius, en els quals s'indiqui, entre altres qüestions, les prohibicions d'ús, la possibilitat de realitzar registres i les eines de control que seran emprades per vigilar el compliment de les obligacions laborals (art. 87 LOPDGDD, Sentència del Tribunal Suprem de 26 de setembre de 2007, rec. 966/2006 i Sentència del Tribunal Europeu de Drets Humans, de 5 de setembre de 2017, Cas Bărbulescu contra Romania).

Aquests criteris d'utilització han de ser configurats amb la participació de la representació legal de les persones treballadores (art. 87.3 LOPDGDD).

El Tribunal Suprem, en la Sentència núm. 225/2024, de 6 de febrer de 2024 (que confirma la Sentència de l'Audiència Nacional núm. 114/2022, de 22 de juliol de 2022), reconeix que aquesta exigència de participació de la representació legal és també aplicable davant qualsevol especificació, ampliació o restricció dels criteris d'utilització. A més, subratlla que, tot i que la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals no té efectes retroactius, si una empresa canvia els criteris que van ser elaborats abans de l'entrada en vigor de la llei, haurà d'assegurar la participació de la representació legal en la nova redacció d'aquests criteris.

L'Audiència Nacional, en la sentència confirmada pel Tribunal Suprem, també recalca que la participació exigida en la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals és equivalent a la consulta recollida en l'article 64 de l'Estatut dels Treballadors, apartats 5 i 6. Per això, la RLPT tindrà dret a emetre un informe previ sobre la qüestió i a

reunir-se amb l'empresa per contrastar opinions i poder arribar a un possible acord sobre el contingut dels criteris d'utilització.

En aquest supòsit, l'incompliment de l'exigència legal de consulta va comportar la nul·litat de la comunicació dels criteris efectuada a les persones treballadores.

Pot la RLPT negociar garanties addicionals sobre els drets digitals de les persones treballadores?

A través de la negociació col·lectiva, poden ser introduïdes garanties addicionals o normes més específiques que garanteixin la protecció dels drets i llibertats de les persones treballadores en relació amb el tractament de les seves dades personals i la salvaguarda dels seus drets digitals (art. 91 LOPDGDD i art. 88 RGPD).

No obstant això, en principi, no podran ser adoptades clàusules, mitjançant conveni o pacte col·lectiu, en les quals es reconegui que l'empresa no pot emprar les proves obtingudes dels sistemes de control per sancionar una persona treballadora. Aquestes provisions sembla que no són considerades vàlides pels tribunals (Sentència del Tribunal Superior de Justícia d'Aragó núm. 379/2016, de 27 de maig de 2016, confirmada per la Sentència del Tribunal Constitucional núm. 160/2021, de 4 d'octubre). El raonament que comparteixen els tribunals és que les potestats disciplinàries reconegudes a l'empresa són irrenunciables i que els acords adoptats amb els òrgans de representació no poden "blindar" les persones treballadores davant el control empresarial. D'aquesta manera, un pacte en conveni col·lectiu que impedeixi a l'empresa usar els mitjans tecnològics per a finalitats disciplinàries podria ser declarat nul i sense efecte per part dels tribunals.

Pot la RLPT denunciar davant la ITSS l'incompliment dels drets d'informació i consulta?

La RLPT, davant la introducció de dispositius tecnològics o el tractament de dades personals en el lloc de treball, disposa dels següents drets d'informació i consulta:

1. Dret d'informació i consulta davant la implementació i revisió de sistemes de control del treball (art. 64.5.f) ET).
2. Dret d'informació algorítmica (art. 64.4.d) ET).

3. Dret de participació (consulta) en l'elaboració dels criteris d'utilització dels dispositius digitals (art. 87.3 LOPDGDD)[2].

4. Dret de consulta sobre la manera d'organització i documentació del sistema de registre de jornada (art. 34.9 ET).

5. Dret d'informació sobre les dades del registre de jornada (art. 34.9 ET).

6. Dret d'informació sobre els riscos identificats en el lloc de treball i les mesures i activitats de protecció i prevenció aplicades (art. 18.1 LPRL).

7. Dret d'informació sobre els mecanismes de prevenció que s'utilitzin a l'empresa (art. 64.2.d) ET).

8. Dret de consulta sobre la implementació de noves tecnologies en el lloc de treball en tot allò relacionat amb les conseqüències que aquestes poguessin tenir per a la seguretat i salut de les persones treballadores (art. 33.1.a) LPRL).

En cas de vulneració d'aquests drets, la RLPT podrà presentar denuncia davant la Inspecció de Treball i Seguretat Social. Entre les infraccions que podrien ser sancionades per la ITSS es troben:

Infraccions en matèria de relacions laborals individuals i col·lectives:

- La transgressió dels drets d'informació, audiència i consulta de la representació de les persones treballadores (art. 7.7 LISOS).

  Es tracta d'una infracció greu que pot ser sancionada amb multa, en el seu grau mínim, de 751 a 1.500 euros, en el seu grau mitjà de 1.501 a 3.750 euros; i en el seu grau màxim de 3.751 a 7.500 euros (art. 40.1.b) LISOS).

Infraccions en matèria de prevenció de riscos laborals:

- L'incompliment dels drets a la informació, la consulta i participació
- Formació i capacitació en competències digitals
- Gènere i participació de les persones treballadores reconeguts en la normativa sobre prevenció de riscos laborals (art. 12.11 LISOS).
- No facilitar a les persones treballadores designades o al servei de prevenció l'accés a la informació i documentació assenyalades en l'apartat 1 de l'article 18 i en l'apartat 1 de l'article 23 de la Llei de Prevenció de Riscos Laborals (art. 12.19 LISOS).

2 La jurisprudència ha considerat que aquest dret de participació equival a la consulta recollida en l'article 64 ET, apartats 5 i 6 (Sentència de l'Audiència Nacional núm. 114/2022, de 22 de juliol de 2022, confirmada per la Sentència del Tribunal Suprem núm. 225/2024, de 6 de febrer de 2024).

Es tracta d'infraccions greus que poden ser sancionades amb multa, en el seu grau mínim, de 2.451 a 9.830 euros; en el seu grau mitjà, de 9.831 a 24.585 euros; i en el seu grau màxim, de 24.586 a 49.180 euros (art. 40.2.b) LISOS):

Pot la RLPT acudir a la jurisdicció social davant un incompliment dels drets d'informació i consulta?

Davant d'un incompliment dels drets d'informació i consulta, la RLPT pot presentar demanda de conflicte col·lectiu (art. 153 LRJS), suplicant que se li faciliti la informació sol·licitada.

L'incompliment dels drets d'informació de la RLPT pot suposar una vulneració de drets fonamentals?

L'incompliment dels drets d'informació recollits a l'Estatut dels Treballadors pot suposar una vulneració de drets fonamentals, concretament del dret a la llibertat sindical, quan l'empresa no transmet la informació demanada als delegats i delegades sindicals, atès que el dret a rebre informació forma part del contingut del dret a la llibertat sindical.

La RLPT pot denunciar davant la Inspecció de Treball i Seguretat Social (ITSS) l'incompliment dels drets d'informació i consulta per part de l'empresa, ja que aquests incompliments poden constituir infraccions sancionables.

Aquesta conclusió va ser adoptada per l'Audiència Nacional, en referència al dret d'informació algorítmica, en la Sentència núm. 101/2025, de 4 de juliol de 2025. Es tracta d'un supòsit en què les seccions sindicals, en base a l'article 64.4.d) ET, havien requerit a l'empresa –que desenvolupava la seva activitat en el sector de *contact center*– informació sobre els paràmetres, regles i instruccions en què es basaven els algoritmes que emprava l'empresa i, concretament, sobre el sistema algorítmic que s'utilitzava per a l'assignació de les lliurances variables a la plantilla. Davant d'aquesta petició, l'empresa respon que no utilitza algoritmes ni sistemes de decisió automatitzada. No obstant això, havent estat aportats indicis de l'ús d'un sistema algorítmic per a l'assignació de les lliurances i els torns, l'Audiència Nacional entén que s'ha produït una vulneració del dret a la llibertat sindical, declara la nul·litat de la pràctica empresarial de no informar i condemna l'empresa a abonar una indemnització de 6.250 euros i a transmetre de manera immediata la informació requerida.

En aquests supòsits, davant una potencial lesió del dret a la llibertat sindical a causa de la inobservança dels drets d'informació i consulta, els sindicats afectats podran presentar demanda de tutela de drets fonamentals expressant els fets que han constituït la vulneració, el dret infringit i la quantia de la indemnització pretesa (art. 183 LRJS). Si queda provada la vulneració del dret a la llibertat sindical, la sentència, d'acord amb les pretensions exercitades, podrà declarar la nul·litat radical de l'actuació empresarial, ordenar el cessament immediat de l'actuació que lesiona drets fonamentals i disposar la reparació del dany causat, entre d'altres (art. 182 LRJS).

Recomanacions i estratègies per protegir les persones treballadores davant el control tecnològic en la negociació col·lectiva

Davant el registre de dispositius electrònics

Acord obligatori sobre la política d'ús dels dispositius electrònics

Com ha estat assenyalat en l'apartat 3 de la guia, la normativa obliga l'empresa a definir una política d'ús dels dispositius electrònics amb la participació de la representació legal. Aquesta participació, en principi, equival a un dret de consulta, per la qual cosa l'empresa haurà de recaptar l'opinió de la representació legal però no necessàriament arribar a un acord.

El conveni col·lectiu pot reforçar aquesta obligació. Es recomana establir que aquesta política no pugui ser decidida unilateralment per l'empresa. La política d'ús hauria de ser **negociada i acordada** amb la representació de les persones treballadores.

D'aquesta manera es garanteix que les normes siguin clares, conegudes i acceptades per tota la plantilla.

Restricció estricta de les causes que justifiquen el control

Segons la normativa, l'empresari solament podrà accedir al contingut dels dispositius digitals facilitats a les persones treballadores per a controlar el compliment de les obligacions laborals o estatutàries o per a garantir la integritat dels dispositius (explicació recollida en l'apartat 2.4 de la guia).

El conveni pot limitar en grau més alt els motius pels quals l'empresa pot controlar els dispositius electrònics. El control només hauria d'estar permès en supòsits concrets, com ara:

- Riscos per a la seguretat informàtica.
- Sospites greus i fonamentades d'un ús fraudulent o deslleial.

S'hauria de prohibir qualsevol control generalitzat, preventiu o indiscriminat sobre tota la plantilla pactant expressament la nul·litat de qualsevol prova recollida fora dels supostos pactats.

Prohibició del control permanent o continu

Es recomana prohibir els sistemes de monitorització constant dels dispositius electrònics. El control continu genera una pressió permanent i afecta la intimitat de la persona treballadora. El conveni pot establir que el control sigui sempre puntual, limitat en el temps i vinculat a una causa concreta, pactant expressament la nul·litat de qualsevol prova recollida fora dels supostos pactats.

Prohibició de la intercepció de les comunicacions

El conveni hauria de prohibir expressament qualsevol control que impliqui interceptar comunicacions. Això inclou:

- Correus electrònics.
- Xats interns.
- Converses amb companys o clients.

Podría pactarse al conveni que la lectura, escolta o supervisió del contingut de les comunicacions de la persona treballadora sols pot efectuar-se mitjançant autorització judicial.

Protecció reforçada davant sistemes basats en intel·ligència artificial

El conveni pot aclarir que la prohibició d'interceptar comunicacions s'aplica també als sistemes automatitzats. Això inclou eines d'intel·ligència artificial que analitzen correus, xats, veu o comportaments digitals sense intervenció humana.

Pot pactar-se expressament al conveni col·lectiu que aquestes tecnologies no s'utilitzin per vigilar o avaluar la persona treballadora de manera automàtica. Aquestes tecnologies poden ser especialment intrusives perquè poden recopilar i analitzar una gran quantitat de dades mentre que la persona treballadora desconeix com estan sent examinades les seves comunicacions.

Registre dels dispositius electrònics existents a l'empresa

La llei obliga l'empresa a elaborar uns criteris d'ús dels dispositius electrònics amb la participació de la representació legal, i a informar del seu contingut a les persones treballadores. Aquests criteris, tal com s'explica en l'apartat 2.4 de la guia, hauran d'indicar almenys les prohibicions d'ús absolutes o parcials, la possibilitat que l'empresa realitzi un registre dels dispositius amb finalitats de control i les eines de control que podrien ser emprades per l'empresa.

Per a garantir una major transparència i seguretat en l'ús dels dispositius digitals en l'empresa i facilitar que la representació legal pugui exercir les seves funcions de control del compliment de la normativa, el conveni col·lectiu pot exigir que, juntament amb els criteris d'utilització, l'empresa tingui l'obligació de crear un **registre** dels dispositius electrònics utilitzats al lloc de treball. Aquest registre hauria d'indicar almenys:

- Els tipus de dispositius.
- Les funcions tècniques.
- La capacitat de control de l'activitat laboral.
- La possible recollida de dades personals sensibles.

La **representació legal** de les persones treballadores hauria de tenir **accés** a aquest registre. El registre s'ha **d'actualitzar** sempre que hi hagi canvis.

Ús personal raonable dels mitjans tecnològics

L'empresa, dins dels criteris d'ús dels dispositius digitals que han de ser elaborats, podria decidir prohibir que els dispositius siguin emprats amb finalitats particulars.

Tanmateix, el conveni pot reconèixer el dret a un ús personal moderat dels dispositius de l'empresa. Aquest ús hauria d'estar permès sempre que:

- No afecti la seguretat informàtica.
- No perjudiqui el treball.
- No impliqui un ús abusiu.

Aquesta previsió evita conflictes i s'adapta a la realitat del treball digital actual.

Presència de la representació de les persones treballadores

Segons s'exposa en l'apartat 2.4 de la guia, en principi, l'empresa podrà accedir al contingut dels dispositius digitals quan així estigui previst en els criteris d'ús, existeixi una raó que legitimi el registre i es respecti el principi de proporcionalitat. No obstant això, encara que es compleixin les garanties establertes en la llei, l'accés als dispositius digitals pot constituir una pràctica intrusiva per a la intimitat de les persones treballadores.

Per això, en empreses amb especial risc de control excessiu, el conveni pot introduir **garanties addicionals**. Una d'elles pot ser permetre o exigir la

presència de la **representació sindical** durant els processos de monitorització o revisió dels dispositius electrònics.

Aquesta mesura reforça el principi de proporcionalitat i el control col·lectiu.

Transparència reforçada sobre la política de control

Si bé l'empresa té l'obligació d'informar les persones treballadores sobre els criteris d'utilització dels dispositius digitals, el conveni pot reforçar aquest deure de transparència en dos aspectes:

- Establir com s'ha d'informar la plantilla sobre la política d'ús dels dispositius electrònics.
- Obligar l'empresa a advertir prèviament quan s'activi qualsevol sistema de control.

La informació ha de ser clara, accessible i comprensible per a tothom.

Limitació del tipus de dades que poden ser recollides

Els dispositius digitals poden emmagatzemar informació sensible de les persones treballadores. Per això, el conveni pot establir que l'empresa, quan realitzi un registre dels mitjans electrònics, només pugui recollir les dades estrictament necessàries per a complir amb l'objectiu legítim que persegueix l'accés.

S'hauria de prohibir la recollida de dades sobre:

- Hàbits personals.
- Preferències.
- Estat emocional.

Aquest tipus d'informació no és necessària per a la relació laboral, i l'accés a aquesta per part de l'empresa pot suposar una intromissió en la intimitat de les persones treballadores.

Limitació del temps de conservació de les dades

Atès que la normativa no fixa un termini màxim clar de conservació de les dades, el conveni pot establir-lo. Es podria pactar que les dades obtingudes

mitjançant el control dels dispositius electrònics no s'haurien de conservar més temps que el permès per la prescripció de les infraccions establerta al estatut dels treballadors que es en tot cas de 6 mesos (art. 60 ET)

Prohibició de combinar el control digital amb altres tecnologies invasives

El control dels dispositius digitals pot ser complementat amb altres tecnologies que poden permetre a l'empresa obtenir més dades de les persones treballadores, accedir a informació sensible o automatitzar processos sense intervenció humana.

El conveni hauria de prohibir expressament combinar el control dels dispositius electrònics amb:

- Elaboració de perfils automatitzats.
- Avaluacions automàtiques del rendiment.
- Anàlisi massiva del comportament digital.

La combinació d'aquestes tecnologies genera un control excessiu i desproporcionat sobre la persona treballadora.


UGT.cat

Guia de drets laborals i de prevenció de riscos: IA i vigilància tecnològica

Registre de l'ordinador

2

UGT.cat