

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

EPI's intel·ligents

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

EPIs intel·ligents

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:

Magnífic

Impressió:

Impremta Pagès

Dipòsit legal:

B 11745-2026

Amb el suport de:

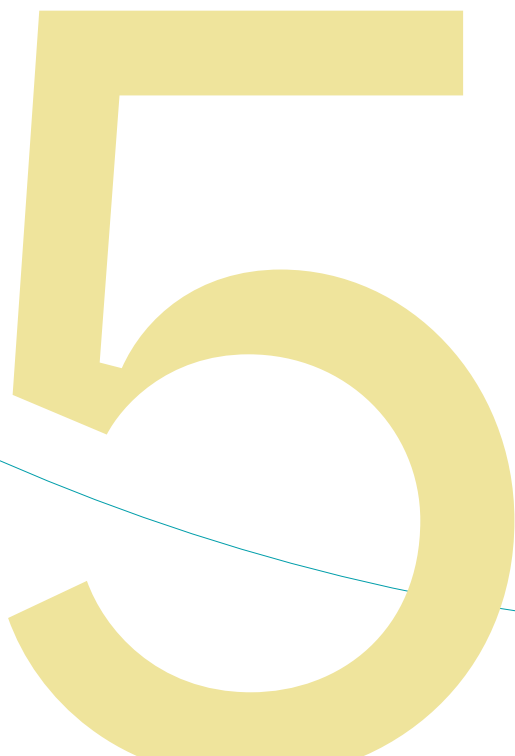


a la feina 



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

EPIs intel·ligents



Taula de continguts

Presentació	6
Introducció	8
Drets individuals en matèria de privacitat i prevenció de riscos laborals	11
• Davant les EPIs intel·ligents	11
Drets col·lectius davant el control tecnològic	23
Recomanacions i estratègies per protegir les persones treballadores davant el control tecnològic en la negociació col·lectiva	28
• Davant l'ús de sensors, EPIs intel·ligents i sistemes d'intel·ligència artificial	28

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 reivindicuem 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 algorismes 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 les EPIs intel·ligents

Què és un EPI intel·ligent?

Un equip de protecció individual (EPI) és qualsevol equip destinat a ser portat o subjectat per la persona treballadora perquè el protegeixi d'un o diversos riscos que puguin amenaçar la seva seguretat o salut en el treball, així com qualsevol complement o accessori destinat a tal fi (art. 4.8º LPRL). L'evolució tecnològica ha donat lloc als anomenats EPIs intel·ligents, que són aquells equips de protecció als quals s'incorporen materials avançats, sensors, dispositius electrònics o sistemes d'intel·ligència artificial, permetent que l'EPI interactuï amb l'entorn o amb la persona treballadora i ofereixi informació, alertes, recomanacions o s'adapti als perills en temps real.

Els EPIs intel·ligents poden recollir i tractar informació molt diversa. En alguns supòsits, es limiten a captar dades no personals, com informació sobre l'entorn (temperatura, gasos tòxics, nivells de soroll, qualitat de l'aire, etc.) o sobre el propi estat de l'EPI (ús correcte, necessitat de manteniment, etc.). En altres supòsits, aquests equips poden recopilar dades personals de la persona treballadora, incloses dades de salut, biomètriques o de localització, i fins i tot processar-les mitjançant sistemes algorítmics o d'IA per detectar riscos, anticipar accidents o formular recomanacions personalitzades. Alguns exemples d'EPIs intel·ligents són els cascos de seguretat que detecten cops, les peces de protecció amb sensors que monitoren constants vitals o els guants que canvien de color al contacte amb substàncies perilloses.

La implantació en el lloc de treball d'aquest tipus d'EPIs, si bé pot augmentar la protecció de la persona treballadora, planteja també importants implicacions

jurídiques. El seu ús haurà de complir, per tant, amb la normativa vigent, tant europea (Reglament (UE) 2016/425, relatiu als equips de protecció individual; Reglament General de Protecció de Dades; Reglament d'Intel·ligència Artificial, etc.) com a nacional (Llei de Prevenció de Riscos Laboral; Reial Decret 773/1997, sobre disposicions mínimes de seguretat i salut relatives a la utilització pels treballadors d'equips de protecció individual, etc.).

Quan podrien implementar-se EPIs intel·ligents?

Els equips de protecció individual que tinguin integrada IA o recopilin dades podran ser implementats quan siguin necessaris per prevenir els riscos identificats en el lloc de treball i garantir la seguretat i la salut de les persones treballadores. L'empresa no podrà introduir aquesta tipologia d'EPIs quan els riscos laborals puguin ser evitats o limitats suficientment per mitjans tècnics de protecció col·lectiva o mitjançant mesures, mètodes o procediments d'organització del treball (art. 17.2 LPRL).

A més, en l'adopció de les mesures preventives, l'empresa haurà de tenir en compte els riscos addicionals que poden implicar i valorar si la magnitud dels riscos introduïts són substancialment inferiors als riscos que es pretén controlar. Només en aquest supòsit es podran adoptar les mesures preventives (art. 15.4 LPRL). Per això, si els EPIs amb IA plantegen nous riscos tant físics com psicosocials que són superiors als riscos que es pretenen prevenir amb la seva incorporació en el lloc de treball no podran introduir-se com a mesura preventiva.

Quin tipus d'EPIs estan prohibits per la normativa vigent?

La normativa sobre prevenció de riscos laborals no prohibeix expressament certes tipologies d'equips de protecció individual, més enllà de considerar que només s'han d'aplicar quan siguin realment necessaris i no plantegin més riscos que els que pretenen controlar (arts. 17.2 i 15.4 LPRL).

Ara bé, quan s'implementen EPIs amb IA integrada o recopilació de dades, són d'aplicació les previsions disposades tant en el Reglament d'Intel·ligència Artificial (RIA) com en el Reglament General de Protecció de Dades (RGPD); per la qual cosa no podran introduir-se en el lloc de treball, EPIs que:

- Tractin categories especials de dades, com les dades de salut o les dades biomètriques dirigides a identificar una persona. L'empresa només podrà utilitzar aquesta tipologia de dades quan acrediti el compliment d'una de les excepcions previstes a l'article 9.2 del RGPD (p. ex., consentiment explícit de la persona treballadora, compliment d'una obligació de Dret laboral, finalitats de medicina preventiva o laboral, etc.).

- Emprin IA i se serveixin de tècniques subliminars, manipuladores o enganyoses amb l'objectiu o l'efecte d'alterar de manera substancial el comportament d'una persona o col·lectiu, minvant de manera apreciable la seva capacitat per prendre una decisió informada i fent que prengui una decisió que provoqui o sigui raonable que provoqui perjudicis considerables a aquesta o altres persones (art. 5.1.a) RIA).
- Utilitzin IA i reconeixin emocions. El Reglament d'Intel·ligència Artificial prohibeix que els sistemes d'IA se serveixin de dades biomètriques, com, p. ex., el rostre o la veu, per distingir o inferir les emocions o les intencions de les persones treballadores; excepte quan la seva implementació respongui a motius mèdics o de seguretat (art. 5.1.f) RIA). L'aplicació en el lloc de treball d'EPIs que integrin sistemes de reconeixement d'emocions podria emmarcar-se en l'excepció prevista pel RIA. No obstant això, en aquests supòsits, s'hauria d'identificar expressament per què és necessària l'aplicació d'aquesta tipologia de sistemes per a la prevenció de riscos laborals i acreditar-se per què no existeix una altra alternativa menys intrusiva que pogués complir amb la mateixa finalitat.
- La Comissió Europea ha assenyalat¹ que l'excepció de motius mèdics o de seguretat ha de ser interpretada restrictivament i que no empara, per tant, la implementació de sistemes de reconeixement d'emocions per controlar el benestar general de les persones treballadores (si pateixen estrès, ansietat, si estan avorrides, etc.) quan no existeix un perill específic que requereixi el monitoratge d'aquest. En aquest sentit, la Comissió ha entès que sí que podria existir un risc si, per exemple, s'empren màquines perilloses i un elevat nivell d'estrès pogués posar en perill la salut de les persones treballadores. En aquests excepcionals supòsits, l'empresa no podria utilitzar les dades amb finalitats diferents, com l'avaluació del rendiment de la persona treballadora.
- En tot cas, el concepte "emocions" inclou només aspectes com la felicitat, la tristesa o la indignació, deixant fora els estats físics, com el dolor o el cansament. Per la qual cosa, els EPIs sí que podrien integrar IA que dedueixi estats físics.
- Emprin IA i recopilin dades biomètriques, p. ex., el rostre o la veu, per deduir o classificar informació sensible de les persones, com la seva raça, religió, orientació sexual, opinions polítiques o afiliació sindical (art. 5.1.g) RIA). Les empreses no poden utilitzar en el lloc de treball EPIs que intentin "endevinar" aquestes característiques i classificar les persones treballadores d'acord amb elles.

1 En les Directrius de la Comissió sobre les pràctiques d'intel·ligència artificial prohibides que s'estableixen en el Reglament (UE) 2024/1689 (Reglament d'Intel·ligència Artificial), publicades el 29/07/2025. Vegeu: <https://ec.europa.eu/newsroom/dae/redirection/document/118659>

S'ha d'informar les persones treballadores quan s'implementen EPIs intel·ligents?

L'empresa haurà d'informar les persones treballadores sobre l'aplicació i utilització d'EPIs intel·ligents en el lloc de treball.

D'una banda, en matèria de prevenció de riscos laborals, l'empresa ha d'adoptar les mesures adequades perquè les persones treballadores rebin informació sobre els riscos laborals per a la seguretat i salut que han estat identificats en el treball i les mesures i activitats de protecció aplicables als riscos assenyalats (art. 18.1 LPRL). Per tant, l'empresa haurà d'informar les persones treballadores sobre la implementació d'EPIs intel·ligents, en tractar-se de mesures de protecció enfront dels riscos laborals.

Més concretament, el Reial decret 773/1997, sobre disposicions mínimes de seguretat i salut relatives a la utilització pels treballadors d'equips de protecció individual disposa que l'empresa haurà d'informar les persones treballadores, prèviament a l'ús dels EPIs, dels riscos contra els quals els protegeixen i de les activitats o ocasions en les quals s'han d'utilitzar; una informació que haurà de ser transmesa en un format que sigui comprensible per a les persones treballadores. A més, l'empresa haurà de proporcionar-los instruccions, preferentment per escrit, sobre la forma correcta d'utilitzar-los i mantenir-los (art. 8.2).

D'altra banda, si es tracta d'equips de protecció individual que incorporen IA, serà d'aplicació el deure d'informació recollit en el Reglament d'Intel·ligència Artificial. Quan es tracti d'un sistema d'IA d'alt risc, l'empresa, abans de posar-lo en servei o d'utilitzar-lo en el lloc de treball, haurà d'informar les persones treballadores afectades que estaran exposades a la utilització d'aquest sistema (art. 26.7 RIA).

L'empresa ha d'informar les persones treballadores sobre l'ús d'EPIs intel·ligents i els riscos associats, incloses les instruccions d'ús. Si incorporen IA d'alt risc, també s'ha d'informar abans de la seva utilització al lloc de treball.

Finalment, si els EPIs recopilen dades personals de les persones treballadores, l'empresa haurà de respectar el dret d'informació establert en el Reglament General de Protecció de Dades, concretament en els articles 12, 13 i 14. En aquest sentit, les persones treballadores hauran de ser informades sobre les finalitats per a les quals es faran servir les dades emprades pels EPIs; les persones destinatàries de la informació; el termini durant el qual es conservarà la mateixa; la possibilitat d'exercir els drets d'accés, rectificació, supressió i limitació del tractament; i la identitat i dades de contacte de la persona responsable del tractament i de la persona designada com a delegada de protecció de dades (art. 14 RGPD). Aquesta informació haurà de ser comunicada de manera concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill (art. 12.1 RGPD); i haurà de ser facilitada per escrit o per altres mitjans, inclusivament, si escau, per mitjans electrònics. La informació només podrà ser facilitada verbalment quan ho sol·liciti la persona interessada (en aquest cas, la persona treballadora) i sempre que es demostrï la seva identitat per altres mitjans (art. 12.1 RGPD).

S'ha de consultar la introducció d'EPIs intel·ligents amb les persones treballadores i la RLPT?

L'empresa haurà de consultar les persones treballadores o la RLPT, si l'empresa compta amb representants, l'adopció d'EPIs intel·ligents, en tot allò relacionat amb les conseqüències que aquestes tecnologies poguessin tenir sobre la seguretat i salut de les persones treballadores (art. 33.1.a) LPRL).

A més, les persones treballadores i els òrgans de representació tindran dret a efectuar propostes a l'empresa dirigides a la millora dels nivells de protecció de la seguretat i la salut a l'empresa (art. 18.2 LPRL).

Si s'implementen EPIs intel·ligents, ¿ha de proporcionar l'empresa una formació adequada a les persones treballadores?

L'empresa té el deure de garantir que les persones treballadores reben una formació teòrica i pràctica, suficient i adequada, en matèria preventiva. Aquest deure de protecció sorgeix tant en el moment de la contractació de cada persona treballadora com quan es produeixen canvis en les funcions que són exercides o s'introdueixen noves tecnologies o canvis en els equips de treball (art. 19.1 LPRL). Per això, si l'empresa implementa EPIs intel·ligents, les persones treballadores hauran de rebre formació específica en matèria de prevenció de riscos laborals.

La formació haurà d'estar adaptada al lloc de treball o funció de cada persona treballadora, adaptar-se a l'evolució dels riscos i a l'aparició d'altres de nous i repetir-se periòdicament si fos necessari (art. 19.1 LPRL).

A més, l'empresa haurà d'organitzar sessions d'entrenament per a la utilització d'EPIs, si escau, i especialment quan es requereixi la utilització simultània de diversos EPIs que per la seva especial complexitat així ho faci necessari (art. 8.3 del RD 773/1997).

Finalment, quan s'implementin EPIs amb IA integrada, l'empresa haurà d'adoptar mesures per garantir l'alfabetització en matèria d'IA de les persones treballadores (art. 4 i Considerant 20 RIA). D'aquesta manera, l'empresa haurà d'introduir activitats de formació perquè les persones treballadores afectades adquireixin els conceptes necessaris que els permetin prendre decisions amb coneixement de causa en relació amb els sistemes d'IA.

A banda dels deures d'informació, consulta i formació, quines altres obligacions en matèria de prevenció de riscos laborals té l'empresa quan s'instal·len EPIs intel·ligents?

En termes generals, independentment del tipus d'equip, quan s'implementen EPIs en el lloc de treball, l'empresa té obligacions en matèria de prevenció de riscos laborals, entre les quals es troben (art. 3 del Reial decret 773/1997):

- Determinar els llocs de treball en què les persones treballadores han de fer ús dels EPIs, així com els riscos davant els quals s'ha d'oferir la protecció, les parts del cos que cal protegir i el tipus d'EPI que s'ha d'utilitzar.
- Elegir els EPIs, atenent les condicions del lloc de treball i de la persona treballadora.
- Proporcionar gratuïtament els EPIs a les persones treballadores.
- Vetllar per una adequada utilització i manteniment dels EPIs (que s'efectuï d'acord amb les instruccions de l'empresa fabricant).

Quines condicions han de reunir els EPIs intel·ligents?

D'acord amb el Reial decret 773/1997 sobre disposicions mínimes de seguretat i salut relatives a la utilització pels treballadors d'equips de protecció individual, tots els EPIs han de proporcionar una protecció eficaç, per la qual cosa hauran de (art. 5):

- Respondre a les condicions existents en el lloc de treball.
- Tenir en compte les condicions anatòmiques i fisiològiques i l'estat de salut de la persona treballadora.
- Adequar-se a la persona portadora, després dels ajustos necessaris.

Així, els EPIs intel·ligents hauran d'adaptar-se a la fisionomia de les persones treballadores, per tal d'evitar que la seva utilització provoqui lesions o accidents.

En aquest context, resulta especialment rellevant analitzar el disseny dels EPIs intel·ligents des d'una perspectiva de gènere. Cal tenir en compte que aquests equips poden haver estat concebuts sense considerar adequadament la diversitat corporal i, en particular, les característiques anatòmiques i fisiològiques de les dones. Aquesta manca de consideració pot comportar que l'EPI no s'adapti correctament a la seva fisionomia, generant molèsties, incomoditat o, fins i tot, situacions de risc per a la seva seguretat i salut, i compromentent, en conseqüència, l'eficàcia real de la protecció proporcionada.

Quines implicacions pot tenir per a la salut de les persones treballadores l'ús d'EPIs amb IA integrada o recopilació de dades?

Els equips de protecció individual intel·ligents, que recopilen dades de les persones treballadores o incorporen IA, són mecanismes de protecció que poden contribuir a millorar la seguretat i salut de l'entorn de treball. No obstant això, la seva implementació també pot afavorir l'aparició de nous perills o potenciar els riscos físics i psicosocials ja presents en el lloc de treball.

Els EPIs intel·ligents poden causar accidents o lesions derivats d'un mal funcionament, d'errors en el sistema, de la generació d'informació incorrecta, de la manca d'adaptació de l'equip a les persones treballadores, o de l'excessiva confiança que les persones hi dipositen i que pot provocar que no se supervisin les seves indicacions o no es compleixin la resta de les mesures de prevenció. A més, el constant monitoratge de la persona treballadora, l'excés d'informació, la sobrecàrrega cognitiva o la falta de formació tècnica per poder utilitzar els EPIs intel·ligents són factors de risc psicosocial que poden propiciar l'aparició de patologies com estrès, ansietat o depressió.

En conseqüència, els riscos que puguin comportar els EPIs amb IA integrada o recopilació de dades han de ser avaluats. Quan els perills que plantegin siguin d'una magnitud més alta que els riscos que es pretenen controlar o prevenir amb la seva implementació i/o existeixin mesures preventives alternatives més segures, aquesta tecnologia no podrà ser introduïda en el lloc de treball (art. 15.4 LPRL).

Quines conseqüències pot tenir l'incompliment de la normativa sobre prevenció de riscos laborals?

L'incompliment de la normativa en matèria de prevenció de riscos laborals (deures d'informació, consulta i formació, etc.) pot donar lloc a la comissió d'infraccions que podrien ser sancionades per la Inspecció de Treball i Seguretat Social:

- Infraccions greus amb què 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):
 - No dur a terme les avaluacions de riscos i, si s'escau, les seves actualitzacions i revisions, així com els controls periòdics de les condicions de treball i de l'activitat de les persones treballadores que escaiguin, o no realitzar aquelles activitats de prevenció que facin necessaris els resultats de les avaluacions, amb l'abast i contingut establerts en la normativa sobre prevenció de riscos laborals (art. 12.1.b) LISOS).
 - Incomplir l'obligació d'efectuar la planificació de l'activitat preventiva que derivi com a necessària de l'avaluació de riscos, o no fer el seguiment d'aquesta, amb l'abast i el contingut establerts en la normativa de prevenció de riscos laborals (art. 12.6 LISOS).
 - L'incompliment de les obligacions en matèria de formació i informació suficient i adequada a les persones treballadores sobre els riscos del lloc de treball susceptibles de provocar danys per a la seguretat i salut i sobre les mesures preventives aplicables, llevat que es tracti d'infracció molt greu conforme a l'article següent (art. 12.8 LISOS).
 - L'incompliment dels drets d'informació, consulta i participació de les persones treballadores reconeguts en la normativa sobre prevenció de riscos laborals (art. 12.11 LISOS).
 - L'incompliment de la normativa de prevenció de riscos laborals, sempre que aquest incompliment creï un risc greu per a la integritat física o la salut de les persones treballadores afectades i especialment en matèria de: disseny, elecció, instal·lació, disposició, utilització i manteniment dels llocs de treball, eines, maquinària i equips (art. 12.16.b) LISOS).
 - No facilitar a les persones treballadores designades o al servei de prevenció l'accés a la informació i la 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).

A més, una conducta empresarial que posi en risc la salut de les persones treballadores pot suposar una vulneració del dret a la integritat física i moral (art. 15 CE). En aquests supòsits, les persones treballadores 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 els EPIs recopilen dades personals de les persones treballadores, quines obligacions haurà de complir l'empresa?

Els EPIs intel·ligents poden recopilar dades personals de les persones treballadores (temperatura de la pell, moviment, freqüència cardíaca, etc.). En aquests supòsits, l'empresa haurà d'atendre les obligacions disposades en el Reglament General de Protecció de Dades (RGPD):

- Haurà de complir els principis relatius al tractament de dades personals (art. 5 RGPD).
- Haurà d'acreditar que el tractament és lícit (art. 6 RGPD); i, si escau, quan s'emprin dades especialment protegides, que s'alça la prohibició de tractament de l'article 9 del RGPD.
- Haurà de garantir la seguretat del tractament, aplicant mesures tècniques i organitzatives apropiades a un nivell de seguretat adequat al risc (art. 32 RGPD).
- Haurà de realitzar una avaluació d'impacte relativa a la protecció de dades. L'Agència Espanyola de Protecció de Dades ha inclòs en la seva llista de tractaments que requereixen aquesta avaluació aquells que impliquin "l'ús de categories especials de dades a què es refereix l'article 9.1 del RGPD", "la utilització de noves tecnologies o un ús innovador de tecnologies consolidades [...]" o "l'observació, monitoratge, supervisió, geolocalització o control de l'interessat de forma sistemàtica i exhaustiva, inclosa la recollida de dades i metadades a través de xarxes, aplicacions o en zones d'accés públic [...]".

Per això, l'empresa haurà d'elaborar, amb caràcter previ a la instal·lació d'EPIs amb IA integrada o recopilació de dades, una avaluació d'impacte relativa a la protecció de dades que haurà d'incloure, entre altres aspectes: una avaluació de la necessitat i proporcionalitat de la mesura i dels riscos que tenen sobre els drets de les persones treballadores i una descripció les mesures previstes per afrontar-los (art. 35.7 RGPD).

¿Poden els EPIs recopilar dades de salut de les persones treballadores?

El Reglament General de Protecció de Dades (RGPD) prohibeix el tractament de dades de salut amb caràcter general (art. 9.1 RGPD). Aquesta prohibició, no obstant això, no és d'aplicació quan concorre una de les circumstàncies recollides a l'article 9.2 del RGPD. En aplicació de les excepcions previstes per la norma, les dades de salut podrien ser utilitzades per l'empresa quan el seu tractament sigui necessari per a finalitats de medicina preventiva o laboral i per avaluar la capacitat laboral de la persona treballadora (art. 9.2.h) RGPD).

Així, la Llei de Prevenció de Riscos Laborals reconeix que l'empresa garantirà a les persones treballadores al seu servei la vigilància periòdica del seu estat de salut en funció dels riscos inherents al treball (art. 22 LPRL). Aquesta vigilància requereix el consentiment de la persona treballadora. Tanmateix, el consentiment no s'entén necessari quan, previ informe de la RLPT, els reconeixements mèdics siguin imprescindibles:

- per avaluar els efectes de les condicions de treball sobre la salut de les persones treballadores,
- per verificar si l'estat de salut de la persona treballadora pot constituir un perill per a aquest, per a les altres persones treballadores o per a altres persones relacionades amb l'empresa o
- quan així estigui establert en una disposició legal en relació amb la protecció de riscos específics i activitats d'especial perillositat.

En certes situacions, la implementació d'EPIs que recopilen dades de salut de les persones treballadores (freqüència cardíaca, pressió arterial, temperatura corporal, etc.) podria venir justificada per la necessitat de verificar si l'estat de salut de la persona treballadora pot constituir un perill per a la mateixa o altres persones. Tanmateix, la norma exigeix que s'apliquin proves proporcionals al risc, que causin les menors molèsties a la persona treballadora i que es respecti el dret a la intimitat i a la dignitat de la persona.

Per això, fins i tot en aquests supòsits excepcionals, s'hauria d'acreditar que el monitoratge de l'estat de salut és una mesura proporcional i imprescindible per al compliment d'un fi, que no pot ser assolit per altres mitjans menys invasius. A més, en tot cas, l'empresa hauria de limitar la recopilació de les dades de salut a aquelles que siguin estrictament necessàries per al compliment de les obligacions de prevenció de riscos laborals.

Quines conseqüències pot tenir l'incompliment de la normativa sobre protecció de dades?

En matèria de protecció de dades, davant un incompliment del Reglament General de Protecció de Dades, es podrà presentar reclamació davant l'Agència Espanyola de Protecció de Dades o davant l'Autoritat Catalana de Protecció de Dades (quan els fets denunciats s'atribueixen a una persona o entitat inclosa dins del seu àmbit d'actuació²). Les autoritats podran iniciar un procediment sancionador si consideren que hi ha indicis d'infracció. En aquests supòsits, les sancions que poden ser imposades a les empreses són les següents:

- Multes administratives de 20.000.000 euros com a màxim o d'una quantia equivalent al 4% com a màxim del volum de negoci total anual global de l'exercici financer anterior, i s'optarà per la de més quantia (art. 83.5 RGPD).

Aquestes multes es podran aplicar quan es cometin, entre d'altres, les següents infraccions (art. 72.1 LOPDGDD):

- El tractament de dades personals vulnerant els principis i garanties de l'article 5 del RGPD.
 - El tractament de dades personals sense que es doni alguna de les condicions de licitud del tractament de l'article 6 del RGPD.
 - El tractament de dades personals de les categories de l'article 9 del RGPD sense que es doni alguna de les circumstàncies previstes en aquest precepte.
 - L'omissió del deure d'informar dels articles 13 i 14 del RGPD.
 - L'impediment o l'obstaculització o la no atenció reiterada de l'exercici dels drets establerts als articles 15 a 22 del RGPD.
 - L'incompliment de les resolucions dictades per l'autoritat de protecció de dades.
- Multes administratives de 10.000.000 euros com a màxim o de quantia equivalent al 2% com a màxim del volum de negoci total anual global de l'exercici financer anterior, i s'optarà per la de més quantia (art. 83.4 RGPD).

2 Per a conèixer l'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades, vegeu: <https://apdcat.gencat.cat/es/documentacio/preguntes-freqüents/Ambit-actuacio-Autoritat-Catalana-de-Proteccio-de-Dades/index.html>



Aquestes multes es podran aplicar quan es cometin, entre d'altres, les següents infraccions (art. 73 LOPDGDD):

- La falta d'adopció de mesures tècniques i organitzatives que siguin apropiades per garantir un nivell de seguretat adequat al risc del tractament, d'acord amb l'article 32.1 del RGPD.
- El tractament de dades personals sense haver dut a terme l'avaluació de l'impacte de les operacions de tractament en la protecció de dades personals en els supòsits en què aquella sigui exigible.

A més, una conducta empresarial que suposi una intromissió il·legítima en l'esfera privada de les persones treballadores pot suposar una vulneració del dret a la intimitat i/o del dret a la protecció de dades (arts. 18.1 i 18.4 CE). En aquests supòsits, les persones treballadores 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).

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 LOP-DGDD 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.

Té dret la RLPT a ser informada sobre la implementació de mesures preventives que suposin el tractament de dades personals o l'ús d'IA?

La RLPT ha de ser informada sobre els riscos identificats en el lloc de treball i les mesures i activitats de protecció i prevenció aplicades (art. 18.1 LPRL), dins de les quals s'englobaria la implementació de tecnologies com els controls biomètrics i els sistemes de reconeixement d'emocions per supervisar la salut o els EPIs intel·ligents.

A més, l'Estatut dels Treballadors reconeix el dret de la RLPT a ser informada trimestralment sobre els mecanismes de prevenció que s'utilitzin a l'empresa (art. 64.2.d) ET).

Finalment, els òrgans de representació tindran dret a efectuar propostes a l'empresa dirigides a la millora dels nivells de protecció de la seguretat i la salut a l'empresa (art. 18.2 LPRL).

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)³.
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 denúncia davant la Inspecció de Treball i Seguretat Social. Entre les infraccions que podrien ser sancionades per la ITSS es troben:

3 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).

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 d'Dret 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).

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.

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 explicant 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).

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

Les tecnologies de control poden afectar de manera intensa la intimitat i la dignitat de les persones treballadores. La negociació col·lectiva és una eina clau per establir límits clars i garanties addicionals més enllà del mínim legal. A continuació es formulen recomanacions pensades perquè els sindicats les puguin incorporar als convenis col·lectius de manera clara i comprensible.

Davant l'ús de sensors, EPIs intel·ligents i sistemes d'intel·ligència artificial

Finalitat preventiva i no disciplinària

El conveni col·lectiu hauria d'establir que els sensors, EPIs intel·ligents i sistemes d'IA només es poden utilitzar amb finalitats preventives o de seguretat i salut laboral. No s'haurien d'utilitzar per controlar el rendiment, la productivitat o el comportament disciplinari de la persona treballadora. La tecnologia ha de servir per protegir, no per vigilar. En aquest sentit, és recomanable establir la nul·litat de qualsevol informació obtinguda mitjançant aquests sistemes que sigui perjudicial per a la persona treballadora.

Prohibició de combinar tecnologies de control

El conveni hauria de prohibir la combinació de sensors o EPIs intel·ligents amb altres tecnologies de vigilància.

Això inclou videovigilància, geolocalització, gravació de sons o sistemes de perfilatge. La combinació multiplica l'impacte sobre la intimitat i resulta desproporcionada.

Prohibició d'ús fora de la jornada laboral

El conveni pot establir que cap sensor, EPI intel·ligent o sistema d'IA funcioni fora de la jornada laboral. No s'haurien de recollir dades durant descansos, pauses o temps de desconnexió digital. La protecció del temps personal és essencial.

Formació i capacitació en competències digitals

Com ha estat assenyalat en l'apartat 2.6 de la guia, d'acord amb la normativa europea, s'ha de garantir l'alfabetització digital de les persones que es vegin afectades per l'ús de sistemes d'IA.

Així, el conveni pot reconèixer el deure de l'empresa de formar a la seva plantilla en competències digitals i garantir la seva adaptació tecnològica als entorns de treball en els quals s'empren sistemes algorítmics o d'IA, sensors, EPIs intel·ligents, etc.

D'aquesta manera, es contribuiria a reduir i evitar la bretxa digital i promoure l'adaptabilitat i ocupabilitat de la plantilla.

Acord previ amb la representació de les persones treballadores

La llei reconeix el dret d'informació algorítmica de la representació legal (el contingut del qual és explicat en l'apartat 3 de la guia), però no reconeix el deure de acordar amb la representació la implementació de sistemes algorítmics o que utilitzen IA.

El conveni pot establir que la implantació de tecnologies, com sensors, EPIs intel·ligents o sistemes d'IA, s'hagi de negociar prèviament amb la representa-

ció legal. El conveni, així mateix, podria no permetre la seva introducció unilateral per part de l'empresa.

El conveni pot preveure l'elaboració d'una comissió paritària que tingui competència per a vigilar i controlar el compliment i l'adequació de l'acord.



Registre dels sensors, EPIs intel·ligents i sistemes d'IA

Per a garantir una major transparència i seguretat en l'ús de sistemes intel·ligents en l'empresa i facilitar que la representació legal pugui exercir les seves funcions de control del compliment de la normativa, el conveni pot obligar l'empresa a crear un registre específic que inclogui:

- Tipus de sensors, EPIs intel·ligents o sistemes d'IA.
- Funcions i dades recollides.
- Finalitat preventiva.
- Possible impacte sobre els drets de les persones treballadores.

La representació legal hauria de tenir accés a aquest registre, que s'hauria d'actualitzar periòdicament. El més rellevant seria pactar la vulneració del dret a l'intimitat de les persones treballadores de l'ús de qualsevol sistema de control per part de l'empresa que no consta al registre.

Informació clara i comprensible a la plantilla

Per a garantir una adequada transparència i complementar els drets d'informació reconeguts per la normativa i detallats en l'apartat 2.6 i 2.7 de la guia, el conveni hauria d'obligar l'empresa a informar a la plantilla de manera clara sobre:

- Quins sensors o sistemes s'utilitzen.
- Quines dades recullen.
- Amb quina finalitat.
- Durant quant de temps es conserven les dades.

La informació ha de ser comprensible, sense llenguatge tècnic innecessari. De nou, el més rellevant seria pactar la vulneració del dret a l'intimitat de les persones treballadores de l'ús de qualsevol sistema de control per part de l'empresa que no siga informat a la plantilla de l'empresa.

Avaluació prèvia d'impacte sobre drets

Segons s'ha exposat en els apartats 2.6 i 2.7 de la guia, l'ús de sistemes algorítmics o d'IA, EPIs intel·ligents o sensors en el lloc de treball pot tenir un impacte significatiu en els drets de les persones treballadores. Són tecnologies que poden arribar a ser realment invasives, puix que poden facilitar l'accés a dades personals i sensibles i permetre un monitoratge i observació constant de les persones treballadores.

Per aquesta raó, amb l'objectiu d'analitzar l'impacte que la implementació d'aquestes tecnologies pot tenir sobre les persones treballadores i els seus drets fonamentals, el conveni pot exigir una **avaluació prèvia** dels riscos per a la intimitat i la salut de les persones treballadores abans d'introduir aquests sistemes en el lloc de treball. Aquesta obligació ja existeix regulada en el art. 35 del Reglament General de Protecció de Dades, no obstant això, el conveni podria aclarir l'aplicació de aquest article a tots els supostos d'ús de eines de control tecnològic.

Sense aquesta avaluació, no s'hauria de permetre la seva utilització i pactar expressament que l'ús de tecnologies de control sense la prèvia avaluació implica una vulneració del dret a l'intimitat de les persones treballadores. La representació legal hauria de participar en aquest procés d'avaluació.

L'ús de tecnologies de control algorítmic requereix una avaluació prèvia d'impacte sobre la intimitat i la salut de les persones treballadores, amb participació de la seva representació, i no s'hauria de permetre la seva implantació sense aquesta anàlisi.



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

EPI's intel·ligents

5



UGT.cat